The Fourth Annual Report to the
President and the Congress of
the Advisory Panel to Assess
Domestic Response Capabilities
for Terrorism Involving
Weapons of Mass Destruction

IV. Implementing the National Strategy

★ 15 December 2002 ★

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (H.R. 3616, 105th Congress, 2nd Session) (October 17, 1998). That Act directed that a federally funded research and development center (FFRDC) provide research, analytical, and other support to the Advisory Panel during the course of its activities and deliberations. RAND has been providing that support under contract from the Department of Defense through one of its FFRDCs, the National Defense Research Institute, since the Advisory Panel's inception.

About RAND

RAND's mission is to improve policy and decisionmaking through research and analysis. Though RAND confronts different policy challenges over time, its principles remain constant. RAND research and analysis aim to:

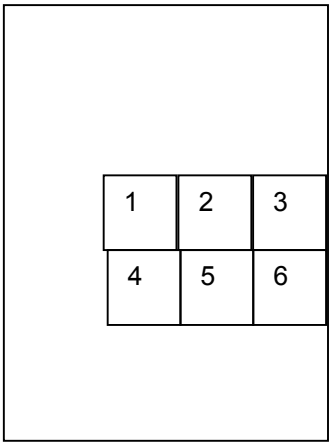
- Provide practical guidance by making policy choices clear and addressing barriers to effective policy implementation.
- Develop innovative solutions to complex problems by bringing together researchers in all relevant academic specialties.
- Achieve complete objectivity by avoiding partisanship and disregarding vested interests.
- Meet the highest technical standards by employing advanced empirical methods and rigorous peer review.
- Serve the public interest by widely disseminating research findings.

FOURTH ANNUAL REPORT TO
THE PRESIDENT AND THE CONGRESS OF THE
ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE
CAPABILITIES FOR TERRORISM
INVOLVING WEAPONS OF MASS DESTRUCTION

IV. IMPLEMENTING THE NATIONAL STRATEGY

15 December 2002

PHOTO CREDITS FROM COVER PAGE



1—Recruits prepare to battle a simulated fire in a Fairfax Count, Virginia, Fire Department training exercise. Photo courtesy of Fire and Rescue Department, Fairfax County, VA
2—FEMA/NY State Disaster Field Office personnel meet to coordinate federal, State and local disaster assistance programs. Photo by Andrea Booher/FEMA News Photo
3—New Mexico Urban Search and Rescue team leader discusses shoring methods with team during exercise. Photo by Andrea Booher/FEMA News Photo
4— Police Special Operations Unit during a VX Nerve Gas terrorist attack training exercise in the city of Glendale, California. Photo courtesy of Graham Owen, photographer, www.grahamowen.com
5—Firefighters being decontaminated at an exercise of responders in Gadsden County, Florida, to test the Terrorism Annex to the county's Comprehensive Emergency Management Plan. Photo courtesy of Capital Area Chapter, American Red Cross
6— NY-TF1 Incident Support Team Medical Unit Leader coordinating with local hospitals for triage of patients during exercise. Photo by Kevin Molloy/FEMA News Photo

THE ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION

December 15, 2002

To Our Readers:

I am pleased to provide this *Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*. The Advisory Panel was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105-261.

In the fifteen month's since the murderous terrorist attacks were perpetrated on American soil, our nation has undergone a transformation. Citizens, governments at all levels, and the private sector continue to adjust to the new threats of terrorism. The effects of September 11, 2001, continue to reverberate throughout America and the World. Some are profound. Others are more subtle.

Considerable progress has been made by an international coalition of countries committed to eliminating the reach and ability of terrorists to inflict wanton destruction targeted against economies, societies, and people. We recognize that the risk will never be completely eliminated. Efforts to enhance preparedness have moved forward so that we can act decisively when attacks inevitably occur. It is clear, however, that actions designed to respond to terrorist attacks; whether conventional, cyber, or those involving weapons of mass destruction, require continuing attention. Achieving a more secure America requires that, as a nation, we better understand the risks we face, and structure the best and most comprehensive ability to prevent, respond, and contain terrorism in the Homeland.

The Advisory Panel was guided by five overarching conclusions this past year:

1. ***The threats we face are not diminishing*** **–** As the pitch of conflict escalates, the threat of an attack on the Homeland is increasing. We must accelerate the pace of preparation to prevent, respond to, and contain an attack.

2. ***Intelligence and information sharing has only marginally improved*** **–** Despite organizational reforms, more attention, and better oversight, the ability to gather, analyze and disseminate critical information effectively remains problematic. The best vehicle must be found to perform the counter-terrorism function and to share information between Federal agencies, the states and localities, and elements of the private sector.

Please address comments or questions to:
RAND
1200 South Hayes Street, Arlington, Virginia 22202-5050 Telephone: 703-413-1100 FAX: 703-413-8111
The Federally-Funded Research and Development Center providing support to the Advisory Panel

3. ***Federal structural changes alone will not significantly improve the security of the homeland*** – The current reorganization in the Federal executive branch will not be a panacea in countering the threat posed by terrorists. In fact these current changes must be carefully implemented and additional actions are needed if we are to be successful. It is imperative that a plan to enable state and local response be designed, funded, implemented, and exercised.

4. ***Measuring performance and sustaining efforts will be key to success*** – Billions of dollars are being committed to countering the terrorist threat. A system must be designed to define priorities, set standards, and measure progress to advance real preparedness.

5. ***Protecting democracy and individual liberties is paramount to achieving ultimate victory*** - Coming through this crisis without diminishing our freedoms or our core values of individual liberty is the entire game. If we pursue more security at the cost of what makes us Americans, the enemy will have won.

If we follow an all-hazards approach to Homeland Defense, we can justify the enormous expenditures coming at the Federal, state, and local levels, and in the private sector. A positive dividend can be reaped as we end up with a better ability to respond to natural disasters and a better public health capacity. Above all, we must remain unified in the same resolve and desire for resolute action that permeated every corner of America in the days and weeks immediately following the September 11, 2001, attacks. We must maintain our drive and momentum to prepare America to defend itself.

The Advisory Panel believes that our fundamental call to service is to inform the national debate on how best to achieve greater safety and security for America. The Advisory Panel will now enter our fifth year of service remaining firmly committed to that principle. The leadership of the Congress and the Administration will continue to be essential in implementing the *National Strategy for Homeland Security,* the corresponding structures, and processes that measure success. A Federal strategy is not a national strategy. Our efforts must be accomplished in strong partnership with our states, communities, private sector entities and every citizen. All segments of our readiness must be addressed in a comprehensive and coordinated fashion. All of us together will meet this challenge at this unparalleled time in the history of the United States. When this latest enemy is gone, the United States will remain, and will continue to be the beacon of freedom in a troubled world.

Sincerely,

James S. Gilmore, III
Chairman

CONTENTS

Letter from the Chairman
Contents i
Executive Summary iii
Chapter I. Introduction 1
Milestones of the Last Fifteen Months 1
Extension of the Advisory Panel 2
Summary of Recommendations in the Second Report 2
Summary of Recommendations in the Third Report 4
Chapter II. Reassessing the Threat 7
A Fresh Perspective 8
Trends in Terrorism 9
"Homegrown" Threats 16
The Threat of Unconventional Weapons 19
Conclusion 26
Chapter III. Applying Cross-Cutting Themes 28
Protecting Our Civil liberties 28
Enhancing State and Local Responsibilities 28
Improving Intelligence and Information Sharing 30
Promoting Strategic Communications 30
Enhancing Coordination with the Private Sector 31
Chapter IV. Resourcing the National Effort 34
Rationalizing the Process—States Versus Localities 34
Establishing Appropriate Burden Sharing 36
Ensuring a Central Focus 36
Determining "How Much is Enough" 37
Measuring Effectiveness 37
Chapter V. Organizing the National Effort 38
Assessing the National Strategy 38
General Comments 38
Definitional Issues 39
"Threat and Vulnerability" 39
"Organizing for a Secure Homeland" 39
"Intelligence and Warning" 40
"Border and Transportation Security" 40
"Domestic Counterterrorism" 41
"Protecting Critical Infrastructures and Key Assets" 41
"Defending Against Catastrophic Threats" 41
"Emergency Preparedness and Response" 41
Improving the Strategy and Structure 42
Intelligence Collection, Analysis, and Dissemination 42
Managing Operations 49
Interagency Coordination 50
Legal Authorities 50
The Congress 51
Chapter VI. Improving Health and Medical Capabilities 52
Applying Resources Effectively 53
Establishing and Using Metrics 55
Improving Hospitals and Other Medical Facilities 56
Enhancing Communications 58

Improving Exercises 59
Perfecting Specialized Response Teams 60
Promoting Technical Assistance 60
Increasing Surge Capacity 61
Providing One-Stop Shopping 62
Enhancing Research 62
Enacting Legal and Regulatory Changes 63
Determining Who Is In Charge 64
Establishing Public Communications Strategies 65
Reconciling Interagency Issues 66
Enhancing Pharmaceutical Supplies and Distribution 66
Implementing a Smallpox Vaccine 67
Chapter VII. Defending Against Agricultural Terrorism 68
Improving Resource Allocations 69
Understanding the Threat 70
Enhancing Planning 71
Improving Laboratory Capacity 74
Compensating for Agricultural Losses 75
Promoting Better Education and Training 76
Chapter VIII. Improving the Protection of Our Critical Infrastructure 78
Reconciling Definitional Terms 78
Enhancing Resources and Establishing Appropriate Burden Sharing 79
Improving Information Sharing 80
Determining Appropriate Identification and Access Controls 81
Improving the Roles of the Public At Large 81
Enhancing Cyber Security 82
Accounting for Private Sector Concerns 84
The Need for an Independent Commission 84
Developing Threat Assessments 85
Creating More Effective Cyber Security Policy 86
Enhancing Aviation Security 86
Improving the Security of Dams 87
Using Models and Metrics 87
Chapter IX. Establishing Appropriate Structures, Roles, and Missions for the Department of Defense 88
Understanding the Proper Role of the Military in Homeland Security 88
Providing for the Defense of the Homeland 89
Providing Military Support to Civil Authorities 89
Improving the Structures for Use of the Military 92
Organizing the Defense Civilian Structure 93
Organizing the Military Structure 93
Improving Military Capabilities for Homeland Security 95
Clarifying Posse Comitatus and Other Relevant Statutes 96
Identifying Requirements 97
Enhancing Training 97
Establishing New Capabilities for Military Support to Civil Authorities 98
Improving the National Guard's Role 101

Table of Appendices 108

Appendices

List of Key Recommendations ..... Inside Back Cover

EXECUTIVE SUMMARY

Fifteen months have passed since the murderous terrorist attacks of September 11, 2001 and the subsequent anthrax attacks. U.S. efforts in the war against terrorism have produced measurable dividends. But the vague and shadowy threat of terrorism continues to present unique challenges.

In July of this year, the President approved for release the first *National Strategy for Homeland Security*—a major milestone in the battle against terrorism. The President recently signed legislation creating the Department of Homeland Security—the most significant restructuring of the Federal government in 55 years. Congress also passed and the President signed into law other landmark legislation over the past 15 months, including the USA PATRIOT Act; measures to enhance physical and cyber infrastructure security and preparedness; Federal terrorism insurance legislation; a bill to improve the key function of intelligence; and additional resources and authority for the use of the U.S. Armed Forces to combat terrorism.

The conclusions and recommendations in this report are the result of almost four years of research and deliberation. The Advisory Panel began its work in 1999 by an in-depth consideration of the threats posed to the United States by terrorists. By the second year, the Advisory Panel shifted its emphasis to specific policy recommendations for the Executive and the Congress and a broad programmatic assessment and functional recommendations for consideration in developing an effective national strategy. In its third report, the panel continued its analysis of critical functional areas. At the time of this publication, 66 of the 79 substantive recommendation made by the panel have been, at this writing, adopted in whole or in major part.

In the National Defense Authorization Act for 2002, the Congress extended the tenure of this Advisory Panel for two years. Thus, we continue our work to contribute to the implementation of a truly effective national strategy for combating terrorism. Because of the attacks in the fall of 2001, and other events that have since unfolded, we felt it was necessary to reexamine the threat assessment of the first report. We then considered several cross cutting themes and applied an analysis of these themes to most, if not all of the functional areas. These themes are: Protecting Our Civil liberties; Enhancing State and Local Responsibilities; Improving Intelligence and Information Sharing; Promoting Strategic Communications; and Enhancing Coordination with the Private Sector. This year we make policy recommendations in five specific areas: Organizing the National Effort; Improving Health and Medical Capabilities; Defending Against Agricultural Terrorism; Improving the Protection of Our Critical Infrastructure; and Establishing Appropriate Structures, Roles, and Missions for the Department of Defense.

Organizing the National Effort

The new threat environment requires the consolidation in one entity of the fusion and analysis of foreign-collected and domestically-collected intelligence and information on international terrorists and terrorist organizations threatening attacks against the United States. ***We recommend that the President direct the establishment of a National Counter Terrorism Center (NCTC).***

The FBI's long standing law enforcement tradition and organizational culture persuade us that, even with the best of intentions, the FBI cannot soon be transformed into an organization dedicated to detecting and preventing terrorist attacks. It is also important to separate the intelligence collection function from the law enforcement function to avoid the impression that the U.S. is establishing a kind of "secret police." ***We recommend that the collection of intelligence and other information on international terrorist activities inside the United States, including the authorities, responsibilities and safeguards under the Foreign Intelligence Surveillance Act (FISA), which are currently in the FBI, be transferred to the NCTC.***

Focused and effective Congressional oversight of the domestic collection and analysis functions is required. Currently, the oversight of the FBI's FISA and other domestic intelligence activities is split between the Judiciary and Intelligence committees in each House of Congress. ***We recommend that the Congress ensure that oversight of the NCTC be concentrated in the intelligence committee in each House.***

The *National Strategy for Homeland Security* designates various lead or co-lead agencies to perform both strategic and tactical analysis and vulnerability assessments. There is no indication that strategic assessments of threats inside the U.S. will receive dissemination to State and local agencies. ***We recommend that the President direct that the NCTC produce continuing, comprehensive "strategic" assessments of threats inside the United States, to be provided to policymakers at all levels, to help ensure appropriate planning and allocation of preparedness and response resources.***

It appears that the new DHS will have no authority for intelligence collection, limited capability for intelligence analysis, but significant responsibility for threat warnings. ***We recommend that the Congress and the President ensure that the DHS has the authority to levy direct intelligence requirements on the Intelligence Community for the collection or additional analysis of intelligence of potential threats inside the United States to aid in the execution of its specific responsibilities in the area of critical infrastructure protection vulnerability assessments. We further recommend that the Congress and the President ensure that the DHS has robust capability for combining threat information generated by the Intelligence Community and the NCTC with vulnerability information the Department generates in cooperation with the private sector to provide comprehensive and continuing assessments on potential risks to U.S. critical infrastructure.***

The *National Strategy for Homeland Security* does not provide any clarity about the extent to which DHS will be "in charge" of executing a response during or after an attack on some CIP sector; nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one. ***We recommend that the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies.***

The question of who is in charge is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, even after DHS is formed, will be in charge in the event of a biological attack. ***We recommend that the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism***

attack, and specify its responsibilities and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations.

There are numerous Federal interagency coordination structures and several combined Federal/State/local structures. The proliferation of such mechanisms will likely cause unnecessary duplication of effort. ***We recommend that the Assistant to the President for Homeland Security review and recommend to the President, and that the President direct, a restructuring of interagency mechanisms to ensure better coordination within the Federal government, and with States, localities, and the private sector, to avoid confusion and to reduce unnecessary expenditure of limited resources at all levels.***

The creation of DHS and the implementation of the *National Strategy* raise several legal and regulatory issues, not the least of which are quarantine, isolation, mandatory vaccinations, and other prescriptive measures. ***We recommend that the President direct the Attorney General to conduct a thorough review of applicable laws and regulations and recommend legislative changes before the opening of the next Congress.***

The Congress is still not well organized to address issues involving homeland security in a cohesive way. Jurisdiction for various aspects of this issue continues to be scattered over dozens of committees and subcommittees. ***We therefore restate our prior recommendation with a modification that each House of the Congress establish a separate authorizing committee and related appropriation subcommittee with jurisdiction over Federal programs and authority for Combating Terrorism/Homeland Security.***

Improving Health and Medical Capabilities

Officials in public health have indicated that it will take at least a five-year commitment from DHHS, at approximately $1 billion per year, to have a material impact on States and local government preparedness to respond to bioterrorist events. ***We recommend that DHHS continue to provide financial support on the order of $1 billion per year over the next five years to strengthen the public health system in the United States.***

The centralization and simplification of grants processes for public health and medical funds is essential to eliminate confusion and unnecessary redundancies. ***We recommend that DHS coordinate and centralize the access to information regarding funding from various agencies such as DHHS (including CDC), EPA, USDA, and others and simplify the application process.***

There is currently no framework in place for monitoring the States' progress in meeting the objectives of the bioterrorism preparedness cooperative agreements program and for evaluating States' performance with respect to various outcomes. Moreover, there is a general lack of understanding on the part of representatives from State and local governments on precisely what they will be held accountable for and how their programs will be evaluated. ***We recommend that DHHS, in consultation with State, local, and private sector stakeholders, establish and***

implement a formal process for evaluating the effectiveness of investment in State, local, and private preparedness for responses to terrorist attacks, especially bioterrorism.

There are not yet widely agreed upon metrics by which to assess levels of preparedness among the medical and public health workforce. Without baseline data, it is impossible to quantify the gap between the current workforce and a workforce "prepared" to address these issues. ***We recommend that DHHS fund studies aimed at modeling the size and scope of the healthcare and public health workforce needed to respond to a range of public health emergencies and day-to-day public health issues.***

Federal officials requested almost $600 million to improve hospital preparedness for FY03. This level of funding is not sufficient to prepare the nation's 5,000 hospitals to handle mass casualty events, mainly because hospitals, like public health agencies, have responded to fiscal pressures by cutting back on staff and other resources and otherwise reducing "excess capacity." ***We recommend that DHHS conduct a comprehensive assessment of the resources required by the nation's hospital system to respond to terrorism, and recommend appropriate Federal-State-Local-Private funding strategies.***

The CDC needs to provide assistance in coordinating and connecting some of its own laboratory and disease surveillance information systems initiatives. These information systems should be connected to provide circular information flow. ***We recommend that DHHS continue to strengthen the Health Alert Network and other secure and rapid communications systems, as well as public health information systems that generate surveillance, epidemiologic and laboratory information.***

Exercises are critical to ensure adequate training, to measure readiness, and to improve coordination. Resources directed to State and local entities to conduct these exercises have been limited and incentives for cross discipline coordination require strengthening. ***We restate a previous recommendation with a follow on that the Congress increase Federal resources for appropriately designed exercises to be implemented by State, local, private sector medical and public health and emergency medical response entities.***

There is an urgent need to clarify the role and functions of the various Federal and State emergency response teams and the extent to which their roles will be coordinated at the Federal, State, and local levels. ***We recommend that DHHS clearly articulate the roles, missions, capabilities and limitations of special response teams; that a plan be developed for the effective integration of such teams; and that focused training for special teams emphasize integration as well as coordination with States and localities.***

State and local officials require technical assistance from the Federal government to select among competing technologies, develop templates for communicating risks and information on actual events to the public, develop plans for surge capacity and pharmaceutical distribution, and provide adequate training to staff. ***We recommend that DHHS evaluate current processes for providing required technical assistance to States and localities, and implement changes to make the system more responsive.***

Some State public health officials are unclear about their role in assisting with planning for the staffing of hospital beds in the state and otherwise becoming involved in surge capacity issues. States are implementing a wide range of preparedness activities but have had little opportunity to share this information with colleagues in other States. ***We recommend that DHHS develop an electronic, continuously updated handbook on best practices in order to help States and localities more effectively manage surge capacity, the distribution of the National Pharmaceutical Stockpile, and other preparedness goals.***

In addition to the substantial research NIH is performing on prevention, treatment, and cures for bioterrorism agents, additional basic research and further research on the application of new technologies is urgently needed. ***We recommend that NIH, in collaboration with CDC, strengthen programs focusing on both basic medical research and applied public health research, and the application of new technologies or devices in public health; and that DHS and OHS, in cooperation, prioritize and coordinate research among NIAID, other NIH entities, and other agencies conducting or sponsoring medical and health research, including DoD, DOE, and USDA, to avoid unnecessary duplication.***

The Model Health Powers Emergency Act would give State authorities certain important powers in a public health emergency. ***We recommend that each State that has not done so either adopt the Model Health Powers Emergency Act, as modified to conform to any single State's special requirements, or develop legislation of its own that accomplishes the same fundamental purposes; and work to operationalize laws and regulations that apply to CBRN incidents—naturally occurring, accidental or intentional, especially those that may require isolation, quarantine, emergency vaccination of large segments of the population, or other significant emergency authorities.***

During investigations into potential bioterror events, there is often a conflict between the goals and operating procedures of health and medical officials on the one hand and public safety officials on the other. The Federal Health Insurance Portability and Accountability Act (HIPAA) is in part designed to keep information about patients confidential and defines narrowly the information and the circumstances under which that information can be released. ***We recommend that the Congress clarify the conditions under which public health agencies, EMS, and hospitals can share information with law enforcement officials in special emergency circumstances under HIPAA. We further recommend, as a prerequisite for receiving Federal law enforcement and health and medical funds from the Federal government, that States and localities be required to develop comprehensive plans for legally-appropriate cooperation between law enforcement and public health, EMS and hospital officials.***

The development of a clear Federal strategic communications strategy, in coordination with State and local medical, public health, and elected officials, is not evident. ***We recommend that DHHS, in coordination with DHS, develop an on-going, well coordinated strategy for education of the public on the prevention, risks, signs, symptoms, treatments, and other important health and medical information before, during and after an attack or large-scale naturally occurring outbreak occurs.***

There is still a lot to learn about the most effective ways to treat people with mental or emotional problems following a terrorist attack. ***We recommend that DHHS, through the National Institute of Mental Health, and in collaboration with CDC, enhance funding for research into the prevention and treatment of the short and long-term psychological consequences of terrorist attacks.***

In-house health and medical expertise in the intelligence community is not sufficiently robust to provide for continuing strategic assessments of bioterrorism cause and effect. ***We recommend that the Intelligence Community improve its capacity for health and medical analysis by obtaining additional expertise in the medical and health implications of various terrorist threats.***

A number of States came up short in their cooperative agreement proposals with respect to their plans for National Pharmaceutical Stockpile receipt and distribution. Federal technical assistance is needed by State and local health officials to develop and exercise these plans. ***We recommend that DHHS significantly enhance technical assistance to States to help develop plans and procedures for distributing the NPS, continue to require exercises that demonstrate the States' ability to employ the NPS, and use specific metrics for evaluating States' capabilities.***

The timely research, development, production, and distribution of certain critical vaccines and other medical supplies continue to be perplexing problems. ***We recommend that DHHS, in collaboration with DHS and DoD, establish a national strategy for vaccine development for bioterrorism which will be consistent with the nation's needs for other vaccines.***

Recently, Federal health officials recommended a multiphase smallpox vaccination program for at-risk emergency medical personnel, with the Federal government assuming liability for adverse events related to vaccination. ***We recommend that the smallpox vaccination plan be implemented in incremental stages with careful analysis and continuous assessment of the risks of the vaccine. We further recommend that DHHS place a high priority on research for a safer smallpox vaccine.***

Defending Against Agricultural Terrorism

There is a lack of an overarching appreciation of the true threat to America's agriculture. Without a broad threat assessment, it is difficult to prioritize resources to counter the terrorist threat. ***We recommend that the President direct that the National Intelligence Council, in coordination with DHS, USDA and DHHS, perform a National Intelligence Estimate on the potential terrorist threat to agriculture and food.***

The Animal Health Emergency Preparedness Plan provides a guide for comprehensive emergency management plans for the response to emergencies involving animals and the animal industry segment of production agriculture. The Emergency Support Function (ESF) in the Animal Health Emergency Preparedness Plan is not currently applicable to any ESF in the Federal Response Plan. ***We recommend that the Assistant to the President for Homeland Security ensure that an Emergency Support Function for Agriculture and Food, consistent***

with the intent of the ESF described in the Animal Health Emergency Preparedness Plan, be included in the Federal Response Plan and the National Incident Response Plan under development.

There are only two existing civilian biosafety level 4 (BSL 4) laboratories for working with and diagnosing the most hazardous animal pathogens. If a large-scale outbreak of a foreign animal disease occurs in the United States, these would provide insufficient capacity. Capabilities at the State level would increase the ability to detect foreign animal diseases early. ***We recommend that the President propose and that the Congress enact statutory provisions for the certification under rigid standards of additional laboratories to test for Foot and Mouth Disease and other highly dangerous animal pathogens.***

Without advance training, and the appropriate equipment and security in place prior to an outbreak, it is not likely that State veterinary labs will be adequately prepared to respond to a crisis. ***We recommend that the Secretaries of Homeland Security and Agriculture (consistent with the November 2001 resolution of the United States Animal Health Association) jointly publish regulations implementing a program to train, equip, and support specially designated, equipped, secure, and geographically distributed veterinary diagnostic laboratories to perform tests and enhance surveillance for agricultural diseases that are foreign to the United States.***

To encourage reporting of diseases and to ensure the stability of the agricultural sector, it is critical that a consistent scheme of national compensation is in place to provide financial assistance to producers and other agribusiness interests impacted by an animal disease outbreak. ***We recommend that the Secretary of Agriculture, in consultation with State and local governments and the private sector, institute a standard system for fair compensation for agriculture and food losses following an agroterrorism attack; and that the Secretary of Health and Human Services should develop a parallel system for non-meat or poultry food.***

There are not enough appropriately trained veterinarians capable of recognizing and treating exotic livestock diseases in the United States. Other types of expertise required for dealing with agricultural diseases are lacking. ***We recommend that the Secretary of Agriculture develop and that the Congress fund programs to improve higher education in veterinary medicine to include focused training on intentional attacks, and to provide additional incentives for professional tracks in that discipline. We further recommend that the Secretary of Agriculture, in coordination with States, improve education, training, and exercises between government and the agricultural private sector, for better understanding the agroterrorism threat, and for the identification and treatment of intentional introduction of animal diseases and other agricultural attacks.***

Improving the Protection of Our Critical Infrastructure

Physical and cyber infrastructure protection contains many very sensitive issues of great importance about which objective research and proposals are very difficult to conduct and develop within the political process. We have modified the recommendation in our third report to cover all infrastructures, both physical and cyber. ***We recommend that the***

Congress establish and that the President support an Independent Commission to suggest strategies for the protection of the nation's critical infrastructures.

The lack of a comprehensive assessment of threats to U.S. infrastructures significantly hampers defensive measures and preparedness activities. ***We recommend that the President direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure.***

The continuing bifurcation of policy for the physical and cyber components of CIP has created confusion and resulted in less than effective policy formulation. ***We recommend that the President direct the merger of physical and cyber security policy development into a single policy entity in the White House.***

Progress in meeting airline passenger baggage-screening goals has been slow, and no screening technology will ever be foolproof. Perhaps equally important is the fact that much of the non-passenger cargo on commercial passenger aircraft is not being screened. ***We recommend that DHS elevate the priority of measures necessary for baggage and cargo screening on commercial passenger aircraft, especially non-passenger cargo.***

The security of general aviation aircraft and facilities is thin, where it exists at all. ***We recommend that that DHS, in conjunction with the airline industry, develop comprehensive guidelines for improving the security of general aviation.***

Hydroelectric and other dams on various watercourses present a significant hazard if terrorists find ways to exploit their controls. ***We recommend that DHS make dam security a priority, and consider establishing regulations for more effective security of dam facilities.***

One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics that help explain the value of protective measures in terms that public and private sector decision makers understand. ***We recommend that DHS use the NISAC modeling and analytic capabilities to develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness of various critical infrastructure components.***

Establishing Appropriate Structures, Roles, and Missions for the Department of Defense

NORTHCOM is in a transitional phase between initial operational capability and full operational capability. In its initial structure, NORTHCOM has few permanently assigned forces, and most of them serve as part of its homeland security command structure. The creation of NORTHCOM is an important step toward enhanced civil-military integration for homeland security planning and operations, and could result in an enhancement of homeland security response capabilities. ***We recommend that the Secretary of Defense clarify the NORTHCOM mission to ensure that the Command is developing plans across the full spectrum of potential activities to provide military support to civil authorities, including circumstances when other national assets are fully engaged or otherwise unable to respond, or when the mission requires additional or different military support. NORTHCOM should plan and train for such missions accordingly.***

In our *Third Report*, we recommended that a unified command be created "to execute all functions for providing military support or assistance to civil authorities"—an all-hazards approach. The Advisory Panel is pleased that NORTHCOM will apparently execute *most* of these functions, and further ***we recommend that the NORTHCOM combatant commander have, at a minimum, operational control of all Federal military forces engaged in missions within the command's area of responsibility for support to civil authorities.***

To achieve that clarity, the laws governing domestic use of the military should be consolidated and the Federal government should publish a document that clearly explains these laws. ***We recommend that the President and the Congress amend existing statutes to ensure that sufficient authorities and safeguards exist for use of the military across the entire spectrum of potential terrorist attacks (including conventional, chemical, biological, radiological, and nuclear threats as well as cyber); that the authorities be consolidated in a single chapter of Title 10; and that DoD prepare a legal "handbook" to ensure that military and civilian authorities better understand the legal authorities governing the use of the military domestically in support of civilian authorities for all hazards—natural and manmade.***

No process is clearly in place to identify among the full scope of requirements for military support to civil authorities. ***We recommend that the President direct the DHS to coordinate a comprehensive effort among DoD (including NORTHCOM) and Federal, State, and local authorities to identify the types and levels of Federal support, including military support, that may be required to assist civil authorities in homeland security efforts and to articulate those requirements in the National Incident Response Plan***

Insufficient attention has been planning and conducting military training specifically for the civil support mission. ***We recommend that the Secretary of Defense direct that all military personnel and units under NORTHCOM, or designated for NORTHCOM use in any contingency, receive special training for domestic missions. Furthermore, in those cases where military personnel support civil law enforcement, special training programs should be established and executed.***

There is a question about whether NORTHCOM's commander "combatant command" (COCOM) relationship with the various service component commands is only for the purpose of unity of *homeland defense* authority and responsibility or applies more broadly to all *homeland security* missions, including NORTHCOM's civil support mission. Thus, at this writing, the extent to which the new command will be able to direct new and expanded civil support training and exercises remains unclear. ***We recommend that the Secretary of Defense clarify NORTHCOM's combatant command authority to ensure that Commander NORTHCOM can direct subordinate commands to conduct pre-incident planning, training, and exercising of forces required to conduct civil support missions.***

Rapid response-type capabilities should arguably be tailored to deal with homeland terrorist events that overwhelm State and local capabilities. ***We recommend that the Combatant Commander, NORTHCOM, have dedicated, rapid-reaction units with a wide range of response capabilities such as an ability to support implementation of a quarantine, support crowd control activities, provide CBRNE detection and***

decontamination, provide emergency medical response, perform engineering, and provide communication support to and among the leadership of civil authorities in the event of a terrorist attack.

States may have difficulty funding homeland security training and operations of the National Guard in State Active Duty status, especially if their missions are conducted for extended periods. Commanders are not clearly authorized under Title 32 to expend Federal funds for training for civil support tasks. ***We recommend that the Congress expressly authorize the Secretary of Defense to provide funds to the governor of a State when such funds are requested for civil support planning, training, exercising and operations by National Guard personnel acting in Title 32 duty status and that the Secretary of Defense collaborate with State governors to develop agreed lists of National Guard civil support activities for which the Defense Department will provide funds.***

The States'existing National Guard military support arrangements must be enhanced to provide for more effective response capabilities in Title 32 duty status. ***We recommend that the President and governors of the several States establish a collaborative process for deploying National Guard forces in Title 32 duty status to support missions of national significance at the President's request; and that the Congress provide new authority under Title 32 to employ the National Guard (in non-Title 10 status) on a multi-State basis, and with governors' consent to conduct homeland security missions, and that the Secretary of Defense define clearly the appropriate command relationships between DoD and the National Guard. We further recommend that the Congress and DoD promote and support the development of a system for National Guard civil support activities that can deploy forces regionally--in coordination with DoD--to respond to incidents that overwhelm the resources of an individual State.***

Further enhancement of the National Guard's civil support capability and responsibility is necessary. In the Third Report we recommended "that the Secretary of Defense … direct that National Guard units with priority homeland security missions plan, train, and exercise with State and local agencies," be expanded. ***We now recommend that the Secretary of Defense direct that certain National Guard units be trained for and assigned homeland security missions as their* exclusive *missions (rather than primary missions as stated in our* Third Report*) and provide resources consistent with the designated priority of their homeland missions.***

CHAPTER I. INTRODUCTION

Milestones of the Last Fifteen Months

Fifteen months have passed since the murderous terrorist attacks of September 11, 2001 and the subsequent anthrax attacks. We have been fortunate, indeed, that no additional, major terrorists attacks have been perpetrated inside our borders. But now is certainly no time to let down our guard.

The ability of al Qaeda and its cohorts may have been significantly degraded but it has not been destroyed. Terrorists linked with al Qaeda continue to carry out highly lethal attacks against Western targets around the world. Recent attacks in Bali, in Kenya, in Tunisia, and on the French tanker off the coast of Yemen, are examples of the work of that far-flung conspiracy and its continuing ability to kill people in large numbers. Intelligence sources continue to pick up "chatter" that indicates more attacks inside the United States are being planned. Some will certainly occur.

U.S. efforts in the war against terrorism have produced measurable dividends. Supported by our allies, we have overthrown the outlaw Taliban regime in Afghanistan, and have had marked success in killing or capturing numbers of al Qaeda followers and some key members of its leadership, including Mohammad Atef, Abu Zubaydah, Omer Farouk, Ramzi Binalshibh, Emad Abdewalid Ahmed Alwan, Abdl Rahman Nashiri, and Qaed Senyan al-Harthi. Yet others—including Ayman al-Zawahiri, reputed to be the number two man in the al Qaeda network—remain at large amid new evidence to suggest that Osama bin Laden himself may still be alive.

Moreover, the vague and shadowy threat of terrorism continues to present unique challenges. After more than fourteen months since the anthrax attacks claimed five lives, injured twelve others, and frightened countless thousands, no arrests have been made in that case.

In July, the President approved for release the first *National Strategy for Homeland Security*—a major milestone in the battle against terrorism. The President recently signed legislation creating the Department of Homeland Security—the most significant restructuring of the Federal government in 55 years.

During this period, Congress also passed and the President signed into law other landmark legislation, including:

- the USA PATRIOT Act, which enhances law enforcement against terrorists;
- Federal terrorism insurance legislation;
- measures to enhance the nation's port security;
- aviation security legislation, including the new Transportation Security Administration;
- a $4.6 billion bioterrorism preparedness program;
- an intelligence bill that attempts to strengthen coordination among agencies and that established the National Commission on Terrorist Attacks Upon the United States to examine the circumstances of the September 11 attacks;
- a $903 billion program for enhancing cybersecurity; and
- additional resources and authority for the use of the U.S. Armed Forces to combat terrorism.

Despite the successes and the changes to law, policy, and the level of resources dedicated to the effort, significant additional improvements, across a broad spectrum of functions, remain to be accomplished.

Extension of the Advisory Panel

In the National Defense Authorization Act for 2002, the Congress extended the tenure of this Advisory Panel for two years with the requirement to submit two additional reports to the President and the Congress on December 15 of 2002 and 2003.[1]

The conclusions and recommendations in this report are the result of almost four years of constant research and deliberation. The Advisory Panel began its work in 1999 with an in-depth consideration of the threats posed to the United States by terrorists, both individuals and organizations. A key finding in the first annual report was the urgent need for a comprehensive national strategy for combating terrorism.

By the second year, the Advisory Panel shifted its emphasis to specific policy recommendations for the Executive and the Congress and a broad programmatic assessment and functional recommendations for consideration in developing an effective national strategy. In its third report, the panel continued its analysis of critical functional areas.

To understand the key conclusions and recommendations in this fourth annual report, it is important to place the recommendations in the context of our previous research and analysis. We begin, therefore, with a brief summary of the recommendations contained in our Second and Third Annual Reports.

While 66 of the 79 substantive recommendations made by the panel have been, at this writing, adopted in whole or in major part, it has never been our intention to offer all the answers or necessarily the best answers for the daunting challenges that we face. Our recommendations are, nevertheless, based on the cumulative experience of our members, informed by exceptionally valuable research and analysis from our support staff at RAND, and are offered in the belief that they can contribute materially to the critical, continuing debate.

Summary of Recommendations in the Second Report

The capstone recommendation in the S*econd Report* was the need for a comprehensive, coherent, functional national strategy: ***The President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.*** As part of that recommendation, the panel identified the essential characteristics for a national strategy:

- It must be truly *national* in scope, not just Federal.
- It must be comprehensive, encompassing the full spectrum of *deterrence, prevention, preparedness, and response* against domestic and international threats.
- Domestically, it must be *responsive to* requirements from and fully *coordinated with State and local officials* as partners throughout the development and implementation process.
- It should be *built on existing emergency response systems*.

[1] See Appendix A.

- It must *include all key functional domains*—intelligence, law enforcement, fire services, emergency medical services, public health, medical care providers, emergency management, and the military.
- It must be *fully resourced* and based on *measurable performance.*

The Second Annual Report included a discussion of more effective Federal structures to address the national efforts to combat terrorism. We determined that the solutions offered by others who have studied the problem provide only partial answers. The Advisory Panel has attempted to craft recommendations to address the full spectrum of issues. Therefore, we submitted the following recommendation: ***The President should establish a senior level coordination entity in the Executive Office of the President***. The characteristics of the office identified in that recommendation include:

- Director appointed by the President, by and with the advice and consent of the Senate, at "cabinet-level" rank
- Located in the Executive Office of the President
- Authority to exercise certain program and budget controls over those agencies with responsibilities for combating terrorism
- Responsibility for intelligence coordination and analysis
- Tasking for strategy formulation and implementation
- Responsibility for reviewing State and local plans and to serve as an information clearinghouse
- An interdisciplinary Advisory Board to assist in strategy development
- Multidisciplinary staff (including Federal, State, and local expertise)
- No operational control

We included a thorough explanation of each of these characteristics in our Second Annual Report.

To complement our recommendations for the Federal executive structure, we also included the following recommendation for the Congress: ***The Congress should establish a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—to address authority and funding, and to provide congressional oversight, for Federal programs and authority for combating terrorism.*** The philosophy behind this recommendation is much the same as it is for the creation of the office in the Executive Office of the President. There needs to be a focal point in the Congress for the Administration to present its strategy and supporting plans, programs, and budgets, as well as a legislative "clearinghouse" where relevant measures are considered. At least 48 committees and subcommittees have some jurisdiction over the issue of terrorism. No existing standing committee can or should be empowered with all of these responsibilities because each existing committee is limited in its jurisdictional scope.

In conjunction with these structural recommendations, the Advisory Panel made a number of recommendations addressing functional requirements for the implementation of an effective strategy for combating terrorism. The recommendation listed below are discussed thoroughly in the Second Annual Report:

Enhance Intelligence/Threat Assessments/Information Sharing

- Improve human intelligence by the rescission of that portion of the 1995 guidelines, promulgated by the Director of Central Intelligence, which prohibits the engagement of certain foreign intelligence informants who may have previously been involved in human rights violations
- Improve Measurement and Signature Intelligence (MASINT) through an expansion in research, development, test, and evaluation (RDT&E) of reliable sensors and rapid readout capability and the subsequent fielding of a new generation of MASINT technology based on enhanced RDT&E efforts
- Review statutory and regulatory authorities in an effort to strengthen investigative and enforcement processes
- Improve forensics capabilities to identify and warn of terrorist use of unconventional weapons
- Expand information sharing and improve threat assessments

Foster Better Planning/Coordination/Operations

- Designate the senior emergency management entity in each State as the *focal point* for that State for coordination with the Federal government for preparedness for terrorism
- Improve collective planning among Federal, State, and local entities
- Enhance coordination of programs and activities
- Improve operational command and control of domestic responses
- The President should always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency

Enhance Training, Equipping, and Exercising

- Improve training through better coordination with State and local jurisdictions
- Make exercise programs more realistic and responsive

Improve Health and Medical Capabilities

- Establish a national advisory board composed of Federal, State, and local public health officials and representatives of public and private medical care providers as an adjunct to the new office, to ensure that such issues are an important part of the national strategy
- Improve health and medical education and training programs through actions that include licensing and certification requirements
- Establish standards and protocols for treatment facilities, laboratories, and reporting mechanisms
- Clarify authorities and procedures for health and medical response
- Medical entities, such as the Joint Commission on Accreditation of Healthcare Organizations, should conduct periodic assessments of medical facilities and capabilities

Promote Better Research and Development and Create National Standards

- That the new office, in coordination with the Office of Science and Technology Policy, develop a comprehensive plan for RDT&E, as a major component of the national strategy
- That the new office, in coordination with the National Institute for Standards and Technology (NIST) and the National Institute for Occupational Safety and Health (NIOSH) establish a national standards program for combating terrorism, focusing on equipment, training, and laboratory processes

Summary of Recommendations in the Third Report

The vast majority of those recommendations for its Third Report were adopted at the panel's regular meeting on August 27 and 28, 2001—two weeks prior to the September attacks. The

Advisory Panel continued to make specific recommendations in key functional areas in order to implement an effective strategy for combating terrorism. The recommendations listed below are discussed thoroughly in that Third Annual Report:

State and Local Response Capabilities

- Increase and accelerate the sharing of terrorism-related intelligence and threat assessments
- Design training and equipment programs for all-hazards preparedness
- Redesign Federal training and equipment grant programs to include sustainment components
- Increase funding to States and localities for combating terrorism
- Consolidate Federal grant program information and application procedures
- Design Federal preparedness programs to ensure first responder participation, especially volunteers
- Establish an information clearinghouse on Federal programs, assets, and agencies
- Configure Federal military response assets to support and reinforce existing structures and systems

Health and Medical Capabilities

- Implement the AMA Recommendations on Medical Preparedness for Terrorism
- Implement the JCAHO Revised Emergency Standards
- Fully resource the CDC Biological and Chemical Terrorism Strategic Plan
- Fully resource the CDC Laboratory Response Network for Bioterrorism
- Fully resource the CDC Secure and Rapid Communications Networks
- Develop standard medical response models for Federal, State, and local levels
- Reestablish a pre-hospital Emergency Medical Service Program Office
- Revise current EMT and PNST training and refresher curricula
- Increase Federal resources for exercises for State and local health and medical entities
- Establish a government-owned, contractor-operated national vaccine and therapeutics facility
- Review and recommend changes to plans for vaccine stockpiles and critical supplies
- Develop a comprehensive plan for research on terrorism-related health and medical issues
- Review MMRS and NDMS authorities, structures, and capabilities
- Develop an education plan on the legal and procedural issues for health and medical response to terrorism
- Develop on-going public education programs on terrorism causes and effects

Immigration and Border Control

- Create an intergovernmental border advisory group
- Fully integrate all affected entities into local or regional “port security committees”
- Ensure that all border agencies are partners in intelligence collection, analysis, and dissemination
- Create, provide resources for, and mandate participation in a “Border Security Awareness” database system
- Require shippers to submit cargo manifest information simultaneously with shipments transiting U.S. borders
- Establish “Trusted Shipper” programs
- Expand Coast Guard search authority to include U.S. owned—not just “flagged”—vessels
- Expand and consolidate research, development, and integration of sensor, detection, and warning systems
- Increase resources for the U.S. Coast Guard for homeland security missions
- Negotiate more comprehensive treaties and agreements for combating terrorism with Canada and Mexico

Cyber Security

- Include private and State and local representatives on the interagency critical infrastructure advisory panel
- Create a commission to assess and make recommendations on programs for cyber security
- Establish a government funded, not-for-profit entity for cyber detection, alert, and warning functions
- Convene a "summit" to address Federal statutory changes that would enhance cyber assurance
- Create a special "Cyber Court" patterned after the court established in FISA
- Develop and implement a comprehensive plan for cyber security research, development, test, and evaluation

Use of the Military

- Establish a homeland security under secretary position in the Department of Defense
- Establish a single unified command and control structure to execute all military support to civil authorities
- Develop detailed plans for the use of the military domestically across the spectrum of potential activities
- Expand training and exercises in relevant military units and with Federal, State, and local responders
- Direct new mission areas for the National Guard to provide support to civil authorities
- Publish a compendium of statutory authorities for using the military domestically to combat terrorism
- Improve the military full-time liaison elements in the ten Federal Emergency Management Agency regions

CHAPTER II. REASSESSING THE THREAT

The attacks of September 11, 2001 reinforced the threat of large-scale attacks inside the United States, and the subsequent anthrax attacks marked the first fatal use of a biological weapon in the United States. This chapter assesses what these and related developments indicate in terms of anti-American terrorism, including the use of chemical, biological, radiological, nuclear, or conventional explosive weapons (CBRNE) inside the United States. Events this past year, including the successful overthrow of the Taliban in Afghanistan, the continuing war on terrorism, and the increasing potential for war with Iraq also carry profound implications for understanding the threat.[2]

In one of its first decisions almost four years ago, the Advisory Panel concluded that, to assess preparedness for terrorist events effectively, one must understand the "full range of potential CBRN threats from terrorists."[3] In 1999, the panel commissioned its supporting staff at RAND, the National Defense Research Institute, to provide an "articulate, comprehensive, and current assessment and analysis of the potential domestic threat from terrorists who might seek to use a CBRN device or agent." The report in 1999 concluded that, although terrorists had an interest in using CBRN weapons to cause mass casualties, significant technological constraints could thwart their malevolent intentions. Accordingly, while not dismissing that potentiality, the panel recommended that the United States must *also* be prepared for higher probability, lower consequence terrorist events—primarily continuing attacks with conventional weapons—which could have specific and unique response requirements of their own.[4] We restate our firm opinion that planning for response to terrorism must not be based primarily on vulnerabilities; that is a misplaced approach. Initially, such planning and preparedness must be based upon a comprehensive analysis of threats before considerations of vulnerabilities.

While the 1995 bombing in Oklahoma City and the 1993 attack on the World Trade Center brought home the potential threat of terrorism, the attacks on September 11 further emphasized that the United States is not immune from foreign attacks of a mass scale on its own soil. It also indicated that, while the United States arguably has other enemies in a number of places, Osama bin Laden and his al Qaeda organization, then based in Afghanistan, posed the greatest threat to this country. In the 15 months since the September 11 attacks, bin Laden and al Qaeda remain the preeminent threat facing the United States today. It should, however, be emphasized that, while the September 11attacks were horrific in terms of the loss of human life and economic damage inflicted on America, it was not the worst-case scenario that many policymakers, government officials, and scholars believed would befall the country either in terms of the

[2] The panel's conclusions are based primarily on a second comprehensive assessment and analysis of potential terrorist threats by RAND staff, supplemented by briefings and other information provided to the panel and from the panel's collective knowledge and experience. This assessment also borrows from an analysis of terrorism and counter terrorism since September 11, 2001 which is summarized in Bruce Hoffman, "Re-Thinking Terrorism and Counterterrorism Since 9/11," *Studies in Conflict and Terrorism*, vol. 25, no. 5 (September – October 2002), pp. 303-316.

[3] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission], *First Annual Report to the President and the Congress*, *I, Assessing the Threat* (Washington, DC: RAND, December 15, 1999), p. vii.

[4] Ibid, pp. 38, 54.

numbers of casualties or even more specifically in the use of exotic or the otherwise unconventional weapons.[5]

A Fresh Perspective

This analysis focuses on changes both in the terrorist environment worldwide and in our nation's sense and perceptions of security since the Advisory Panel's first analysis of the threat. The overall conclusion remains that lower consequence events are of a higher probability than higher consequence events. Nevertheless, the higher consequence events may now be somewhat more probable for a variety of reasons, including:

- The dramatic illustration on September 11 of how terrorists' motives have changed, showing that groups like al Qaeda have as a goal killing large numbers of people;
- The level of sophistication and coordination, patience and determination achieved by al Qaeda in carrying out simultaneous or sequential attacks;
- What we know now about al Qaeda's ambitions to develop chemical, biological, nuclear and radiological weapons; and
- The measure of success, albeit limited, of the anthrax attacks last fall, coupled with the fact that the perpetrator or perpetrators of those attacks have not been found.

For those reasons and others, the nation must be sufficiently prepared to respond to threats across the weaponry and technological spectrum.

We are also compelled to take this new approach because of the discovery of crude biological and chemical weapons capabilities in Afghanistan,[6] the subsequent capture of al Qaeda operatives, as well as the continuing series of lethal bombings overseas such as the attack off Yemen on the French oil tanker, the bombing in Bali, and the attacks in Kenya and in Tunisia—showing once again the agility of al Qaeda and its sympathizers to strike on terms of their own making.

The United States war on terror may have changed the character of the threat itself by forcing terrorists to change tactics and targets. According to Undersecretary of State John Bolton:

> Today, the United States believes that the greatest threat to international peace and stability comes from rogue states and transnational terrorist groups that are unrestrained in their choice of weapon and undeterred by conventional means. The September 11 attacks showed that terrorist groups were much better organized, much more sophisticated, and much more capable of acting globally than we had assumed possible. Our concept of what terrorists are able to do to harm innocent civilians has changed fundamentally. There can be no doubt that, if

[5] See U.S. Senate, Committee on the Judiciary, *Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Hearing, March 27, 2001, Washington: U.S. Government Printing Office, 2001.
[6] David McGlinchey, "Al Qaeda: Coalition Forces Disabled Chemical Plant in 2001," *Global Security Newswire*, September 18, 2002.

> given the opportunity, terrorist groups such as al Qaeda would not hesitate to use disease as a weapon against the unprotected; to spread chemical agents to inflict pain and death on the innocent; or to send suicide-bound adherents armed with radiological explosives on missions of murder.[7]

This chapter first explores general trends in terrorism with a focus on the high-end threat posed specifically by foreign terrorist organizations. It then turns to an examination of the domestic threat both from traditional, U.S. "homegrown" terrorists as well as from citizens and legal residents of the United States working with or influenced by foreign terrorists groups. Finally the chapter focuses on the specific threat of CBRN weapons.

We emphasize that this analysis is only "a snapshot in time." In the future, changes in one of a number of significant factors could cause any threat analysis to be modified and to reach substantially different conclusions.

Trends in Terrorism

First, terrorism has undeniably continued its trend toward increasing lethality. While terrorist groups have consistently targeted U.S. citizens and businesses overseas for the past thirty years, within the span of just an hour and a half on September 11, more than three times the number of Americans were killed than during the entire previous 33 years.[8] Indeed, terrorist groups have conducted approximately 3,300 attacks against U.S. targets since 1968.[9] Yet in all of these attacks no more than some 1,000 total Americans were killed. Similarly, only 14 terrorist operations in the past 100 years have killed more than 100 persons.[10] The attacks on the World Trade Center and the Pentagon, therefore, represent a dramatic increase in the lethality of terrorist attacks. The trend towards intense bloodshed has not subsided. The October 2002 attack in Bali killed approximately 200 people—the deadliest terrorist attack since September 11, 2001. Indeed, it is believed that the Bali incident was intentionally designed to cause maximum casualties.[11] This trend stems in part from changes in terrorists' motivations. Throughout most of the last half of the twentieth century terrorists had a defined set of political, social, or economic objectives. A new generation of terrorists has emerged with different motives and includes millenarian movements and nationalist religious groups whose aims are much more deadly.[12]

---

[7] John R. Bolton, Undersecretary Of State for Arms Control and International Security, "The International Aspects of Terrorism and Weapons of Mass Destruction," Second Global Conference On Nuclear, Bio/Chem Terrorism: Mitigation And Response, The Hudson Institute, Washington, DC, November 1, 2002 as released by the State Department.

[8] Hoffman, "Re-Thinking Terrorism…," p. 304.

[9] Several factors can account for this phenomenon, in addition to America's position as the sole remaining superpower and leader of the free world. These include the geographical scope and diversity of America's overseas business interests, the number of Americans traveling or working abroad, and the many U.S. military bases around the world.

[10] Brian M. Jenkins, "The Organization Men: Anatomy of a Terrorist Attack," in James F. Hoge, Jr. and Gideon Rose, *How Did This Happen? Terrorism and the New War* (NY: Public Affairs, 2001), p. 5.

[11] Maria Ressa, Atika Shubert, et al., "Hundreds missing in Bali bombing," *CNN.com*, October 14, 2002, available at http://www.cnn.com/2002/WORLD/asiapcf/southeast/10/13/bali.blast.missing/, accessed November 6, 2002.

[12] Hoffman, "Lessons of 9/11," p. 4.

Yet "lethality" is not necessarily the only way of measuring the increasingly significant impact that terrorism is having on the United States and the international community. Indeed, terrorist attacks have also inflicted growing economic damage on target societies. It appears that this trend may be the result of a conscious decision on the part of the organizations responsible for either perpetrating or fomenting this violence. For example, Osama bin Laden and other al Qaeda leaders were reportedly elated by the economic losses caused by the September 11 attacks. Bin Laden bragged in the October 2001 videotape declaring war on the United States about the "trillions of dollars" of economic losses. Similarly, Ahmed Omar Sheikh, the chief suspect in the killing of the American journalist, Daniel Pearl, echoed this same point. While being led out of a Pakistani court in March, he exhorted anyone listening to "sell your dollars, because America will be finished soon."[13] Even if al Qaeda did not hold economic damage as a primary objective in the September 11 attacks, these attacks have raised an awareness of how sensitive the U.S. and world economy can be to terrorism. Indeed, bin Laden and his chief lieutenant Ayman al-Zawahiri, in tapes released on October 6, 2002, reportedly reiterated the focus on economic targets. Bin Laden pointedly warned, "By God, the youths of God are preparing for you things that would fill your hearts with terror and target your economic lifeline until you stop your oppression and aggression."[14] And al-Zawahiri similarly echoed this theme, "The settlement of this overburdened account will indeed be heavy. We will also aim to continue, by permission of Allah, the destruction of the American economy."[15]

The second general trend is more recent and, as such, likely the result of the U.S. war on terrorism. Despite a continued desire to execute large scale, high consequence attacks, smaller, more frequent attacks are more likely to occur in the near future. As law enforcement and intelligence services continue to disrupt al Qaeda and its affiliated groups overseas and degrade their capability to conduct mass casualty attacks inside the United States, these groups are likely to turn to smaller-scale alternatives against more accessible, softer targets.[16] Inside the United States, these smaller-scale attacks could in the future take the form, among others, of suicide bombings, assassinations, low level biological attacks, car and truck bombings of government buildings and other symbolic targets, or arson attacks against banks.[17] Indeed, Sheik Hassan Nasrallah, the leader of Hezbollah, recently called for global suicide attacks, although traditionally Hezbollah has only targeted Israelis in the Middle East.[18] It is worth noting, however, that Hezbollah is widely believed to have been responsible for the 1992 and 1994 truck bombings outside the Israeli embassy and then a Jewish community center in Buenos Aires, thereby demonstrating a global terrorist reach.

---

[13] Raymond Bonner, "Suspect in Killing of Reporter Is Brash and Threatening in a Pakistani Court," *New York Times*, 13 March 2002.

[14] Associated Press, "Bin Laden tape: 'Youths of God' plan more attacks," October 7, 2002, available at http://www.smh.com.au/articles/2002/10/07/1033538881353.html on November 3, 2002.

[15] Arena, Kelli, "U.S.: Latest Tapes Cause for Concern," October 10, 2002, available at http://www.cnn.com/2002/WORLD/asiapcf/central/10/08/alqaeda.threat.tape/ on November 3, 2002.

[16] Peter Finn, Dana Priest, "Weaker al Qaeda Shifts To Smaller-Scale Attacks," *Washington Post*, October 15, 2002, and available at http://www.washingtonpost.com/wp-dyn/articles/A25832-2002Oct14.html, accessed October 29, 2002.

[17] Agence France-Presse, "Homeland Security chief sees new al Qaeda attacks in U.S.," August 27, 2002, available at http://www.inq7.net/brk/2002/aug/27/brkafp_2-1.htm, accessed October 29, 2002.

[18] In a recent speech at a rally broadcast on television in Lebanon, Nasrallah stated, "Martyrdom operations - suicide bombings - should be exported outside Palestine. I encourage Palestinians to take suicide bombings worldwide." Paul Martin, "Hezbollah calls for global attacks," *Washington Times*, December 4, 2002.

In conjunction with this, a trend towards softer, or unprotected, targets has also emerged, since September 11, in attacks against Western targets overseas. For example, al Qaeda, in conjunction with its affiliated groups, has conducted attacks against a synagogue in Tunisia (April 2002), a bus carrying French naval engineers in Pakistan (May 2002), a nightclub frequented by Westerners in Bali (October 2002), and an Israeli-owned hotel in Kenya (November 2002). The argument for this general trend was further reinforced in May 2002, when senior al Qaeda lieutenant Abu Zubaydah, currently in U.S. custody, warned that al Qaeda operatives were discussing attacks on soft targets, specifically non-governmental buildings and places where large number of Americans gather.[19] Moreover, another al Qaeda operative in U.S. custody, Indonesian Mohammad Mansour Jabarah, told U.S. investigators, shortly before the tourist attacks on Bali in October that Jemaah Islamiyya operative Hambali was planning to conduct "small bombings in bars, cafes, or nightclubs frequented by Westerners in Thailand, Malaysia, Singapore, the Philippines, and Indonesia."[20]

Third, recent events indicate that terrorists will likely be forced to continue to innovate in the types of attacks they conduct, the methods they use, and the targets they select. Although historically, modern terrorists have been more imitative than innovative, recent attacks by al Qaeda demonstrate that this group, in particular, has proven adept at tactical innovation.[21] For example, al Qaeda's attacks against USS *Cole* demonstrated a degree of innovation, even if it were copying tactics that the Tamil Tigers have successfully used to target naval vessels off the coast of Sri Lanka. More significantly, the attacks of September 11 displayed al Qaeda's ability to employ deception and innovative tactics to successfully attack targets. Since September 2001, it appears that al Qaeda is continuing to identify new U.S. vulnerabilities both at home and abroad, adjusting their tactics and targeting in part as a response to their lack of sanctuary and the need to be more careful in their logistical support activities and communications. For example, press reports have indicated that some al Qaeda operatives have engaged in scuba diver training in order to place explosives on ships in port,[22] while other reports have pointed to threatened attacks on U.S. passenger trains.[23] Further sections of this report will focus on the chemical, biological, radiological and nuclear (CBRN) threats of terrorist groups. Suffice it to say for the moment that in March 2001, Italian authorities obtained evidence suggesting that a terrorist cell affiliated with al Qaeda had contemplated using poison gas in an attack on the U.S. Embassy in Rome. Italian authorities, working with U.S. officials, arrested members of this cell in January 2001.[24] The significance of this plan is the attempt by terrorist cells possibly independent of the organization's command and control to adapt and innovate not only the means of attack but the tactics as well.

Additionally, there appears to be a general trend toward increasing cross-fertilization amongst terrorist groups. It is likely that as the war on terrorism reduces the ability of these groups to

---

[19] Elaine Shannon, "Another warning from Zubaydah," *Time*, May 11, 2002, available at http://www.time.com/time/nation/article/0,8599,236992,00.html, accessed November 12, 2002.
[20] Maria Ressa, "Building al Qaeda's Asian terror network," *CNN.com*, November 7, 2002, available at http://asia.cnn.com/2002/WORLD/asiapcf/southeast/10/29/asia.jihad.2/, accessed November 11, 2002.
[21] Hoffman, "Lessons of 9/11," p. 7.
[22] "Terror alerts on small planes, scuba divers," May, 26, 2002, available at http://www.cnn.com/2002/US/05/26/terror.threats/index.html accessed October, 25,2002.
[23] "FBI Warns of Rail Threat," *CBSNEWS.com*, October 25, 2002, available at http://www.cbsnews.com/stories/2002/10/25/attack/main526923.shtml, accessed November 14, 2002.
[24] Patterns of Global Terrorism, p. 38.

operate, they may begin to share expertise, training, materials, and even participate in each other's operations. This cross-fertilization has occurred in the past with groups such as the Palestine Liberation Organization (PLO), the Provisional Irish Republican Army (PIRA), and the Basque Fatherland and Freedom (ETA). However, al Qaeda's offer to train and equip other Islamic terrorist groups in exchange for their focus on Western targets represents a more concentrated and strengthened level of cross-fertilization. Indeed, terrorist groups in Southeast Asia, such as Jemaah Islamiya (JI), Kumpulan Mujahidin Malaysia (KMM), the Abu Sayyaf Group (ASG), and the Moro Islamic Liberation Front (MILF) in the Philippines illustrate that this type of cross-fertilization can have a significant and enhanced effect on group capabilities. For example, the MILF runs a training camp in the Philippines with funds from al Qaeda that both al Qaeda and the MILF can use to train not only themselves but other foreign terrorist groups, including the JI, in guerilla warfare and terrorism tactics.[25] In addition, a key member of the Abu Sayyaf Group, likely inspired by bin Laden and al Qaeda, was arrested in November 2002 for planning a series of bombings in Manila and the southern Philippines, including an attack on the U.S. Embassy. Two Yemeni nationals reportedly trained this ASG member with ties to the JI in explosive techniques.[26] Even groups that traditionally have not cooperated due to religious differences such as Hamas, al Qaeda, and Islamic Jihad (Sunni Muslim) and Hezbollah (Shiite Muslim) may be working together because their hatred for the West overcomes their dislike of each other. [27]

A fourth trend is the continued evolution of "loose networks." Al Qaeda, for instance has direct influence over both its professional cadre, represented by terrorists such as Mohammed Atta and over the trained amateurs such as Ahmed Ressam,[28] but it also has indirect influence over a much larger group of people that range from local walk ins to like minded insurgents, guerillas and terrorists.[29]

In such cases, group affiliations are not as clear and, therefore, it will be difficult for the U.S. government to determine responsibility for future attacks and response options accordingly. The disrupted terrorist plot against U.S. interests in Singapore in December 2001 is representative of this phenomenon. In this case, a network of extremists from throughout Southeast Asia worked in conjunction with al Qaeda leadership to plan an attack on the U.S. Embassy, a U.S. Navy ship, Navy personnel using the subway, and other facilities.[30] U.S. and Singapore intelligence eventually identified the JI as the primary group responsible. The JI relied heavily on al Qaeda operatives, however, for guidance and support and were acting as proxies of al Qaeda.[31]

---

[25] "MILF denies training camps used by al Qaeda," INQ7.net, September 18, 2002, available at http://www.inq7.net/brk/2002/sep/18/brkpol_10-1.htm, accessed November 20, 2002.
[26] Jess Liwanag, "Philippines arrests al Qaeda linked bomber," *CNN.com,* November 14, 2002, available at http://www.cnn.com/2002/WORLD/asiapcf/southeast/11/14/phil.bomb.suspect/index.html, accessed November 20, 2002.
[27] Hezbollah has recently been meeting in Lebanon with members of Hamas and Islamic Jihad and issuing joint press statements, Martin, December 4, 2002.
[28] Ressam was recruited into al Qaeda and trained in Afghanistan, but he was sent to the United States with open ended targeting instructions, whereas individuals such as Atta received plentiful resources and specific guidance on targets and tactics. Hoffman, "Lessons of 9/11," pp. 13-14.
[29] Local walk ins are local radical Islamic groups that look to al Qaeda for funding of their homegrown ideas. Like minded groups may have benefited from bin Laden's guidance and training and share his anti-American/anti-Western views. Hoffman, "Lessons of 9/11," pp. 14-15.
[30] Patterns of Global Terrorism, pp. 20-21.
[31] Ibid, pp. 20-21.

Videotape was found amongst the rubble of the home of an al Qaeda leader in Afghanistan that showed surveillance footage of the intended targets in Singapore. Handwritten notes in Arabic that accompanied the tape were also discovered and revealed more details about the plot.[32] This indicates that al Qaeda was intimately involved in the target identification and tactical decision-making. Yet what is most interesting about this plot, is that the JI had not previously been identified by policymakers as having an anti-U.S. agenda, again illustrating that loose networks can be difficult to measure in terms of threat salience.[33] Similarly, the string of attacks carried out earlier this year by Pakistani militants against Westerners in Karachi is another example where responsibility was not immediately clear. Because a number of terrorist groups are operating in Kashmir, most with predominantly local agendas, it was difficult to determine the perpetrators of these anti-Western attacks and therefore accurately assess future threats. The militants were eventually identified as belonging to a splinter group of the Harakat ul-Mujahedin (HUM), called the Harakat ul-Mujahedin al-Alami (HUM-A). This splinter group allegedly separated from the HUM because it wanted to focus more on Western, rather than local, targets. This group was responsible for the car bombing of the U.S. Consulate in Karachi in June 2002.[34] Most recently, in the attacks on the Israeli Hotel in Kenya suspicion has fallen on al Qaeda—al Qaeda communiqués have claimed credit[35]—because of the earlier attack on the U.S. embassy in Nairobi in 1998. (But other suspects, such as Al Ittihad al Islami—a Somali group—and Hezbollah, have also emerged.[36])

Indeed, there are a number of loose networks of terrorists forming based on their common hatred of the West. This appears to signal that these organizations support bin Laden's "America first" policy, his goals of ousting pro-Western governments from the Islamic world, and the creation of a transnational Islamic Caliphate. Though the previously mentioned cooperation between Islamic extremist groups in Southeast Asia is the best example of how terrorists who subscribe to this ideology are creating new alliances, several Islamic extremist groups in Central Asia also decided to join forces in September 2002 to create a single Islamic terrorist entity, the Islamic Movement of Uzbekistan (IMU), which has ties to bin Laden, and encompasses separatists from Kyrgyzstan, Tajikistan, Chechnya, and the Xingjiang Province of China.[37]

Despite the fact that some "loose networks" are forming around bin Laden's anti-Western agenda, it is also possible that other terrorist groups will return to their local goals, possibly because they no longer feel that pursuing an anti-Western agenda achieves their objectives or as a result of the pressure of the U.S. war on terrorism. This phenomenon may also indicate a failure on the part of al Qaeda to sell its propaganda of worldwide *jihad* and the restoration of the Islamic Caliphate to localized groups, as well as the success of the war on terror in deterring terrorist adversaries. Although al Qaeda wants groups affiliated with its organization to attack locally, because they know their own immediate environment best and can take responsibility, al

---

[32] Ibid.
[33] Ibid, pp. 20-21, 123.
[34] CDI, "Action Update," Terrorism Project, October 22, 2002, available at http://www.cdi.org/terrorism/actionupdate.cfm, accessed October 29, 2002.
[35] "Al Qaeda Claims Kenya Attacks," December 3, 2002, available at http://uk.news.yahoo.com/021202/140/dfvv0.html; and "Al Qaeda Claims Role in Kenya Attacks," *Washington Post,* December 9, 2002 available at http://www.washingtonpost.com/wp-dyn/articles/A27943-2002Dec8.html
[36] Eric Lichtblau, "Striking 'Soft' Targets Complicates Security," *New York Times*, November 30, 2002.
[37] FBIS, "Russian Newspaper on Union of Islamic Movements in Central Asia," *Moscow Pravda*, September 16, 2002.

Qaeda wants these attacks to target Westerners, particularly Americans, in addition to their own governments. It does not further al Qaeda's global Islamic revolutionary goals for a particular Muslim group to reject the idea of targeting the West and to focus narrowly on obtaining power in Kashmir in isolation from the wider struggle. For example, since September 11, at least two Islamic terrorist groups that had previously been associated with al Qaeda have chosen to reject bin Laden's call for worldwide *jihad*. One of these groups, the HUM in Pakistan moved away from supporting bin Laden after 22 of its operatives were killed in U.S. air raids in Afghanistan, and its assets were frozen, arguably demonstrating the utility of direct pressure in combating terrorism.[38] Groups that turn inward to focus on local goals, however, often spur the formation of more extreme splinter organizations. If these splinter groups can muster resources and support, they can pose a serious threat to Americans and their interests. HUM's decision to reject involvement with al Qaeda sparked a split within the group, and the more violent HUM-A was formed. Since the HUM-A was created, it has conducted a number of attacks against Westerners and Christians in Pakistan, including the bombing of the U.S. Consulate in Karachi in June 2002.

Terrorists are also relying on new technologies, such as email, the Internet, and video/audio production, to enhance internal communications and spread their message to a variety of audiences to enhance recruitment, popular support, and intimidate their adversaries.[39] Although in al Qaeda's case this stems in part from a loss of a dedicated safe haven, it should be noted that this group has always been especially adept at external communications, public relations, and propaganda. While this innovation may increase the danger to Americans by rallying additional support to bin Laden and his cause, it may also provide a vulnerability that can be targeted in the war on terrorism because terrorists have become highly dependent on these communications technologies. Secure email, cell phone calls, and Internet communications have proven largely effective in the short run and have allowed terrorists to maintain the momentum they would surely have lost after the U.S. and allied bombing of Afghanistan last fall, had these technologies not been available for their use. Indeed, al Qaeda leadership has utilized both video and audiotapes more frequently since September 11 to send messages directly to their followers while at the same time also warning their adversaries. For example, Zawahiri gave a taped interview to al-Jazeera news network in October 2002 in which he addressed the U.S. and its allies directly:

> Our message to our enemies is this: America and its allies should know that their crimes will not go unpunished…We advise them to hasten to leave Palestine, the Arabian Peninsula, Afghanistan, and all Muslim countries, before they lose everything.[40]

To his followers, Zawahiri had praise and perhaps an indication of what the next al Qaeda targets might be:

---

[38] "Pakistan Arrests Bomb Mastermind," Associated Press, CBSnews.com, September 18, 2002, available at http://www.cbsnews.com/stories/2002/09/25/world/main523196.shtml, accessed November 14, 2002.
[39] Andrew Higgins, Karby Leggett, Alan Cullison, "How al Qaeda put the Internet to use," *The Wall Street Journal,* November 11, 2002, available at http://www.msnbc.com/news/833533.asp?0si, accessed November 20, 2002.
[40] FBIS, "Al-Zawahiri Says Bin Laden, Mullah Omar 'Enjoy Good Health,' Doha Al-Jazeera Satellite Channel Television Arabic, October 8, 2002.

> The mujahid youths have addressed a message to Germany and another to France. If the measures have not been sufficient, we are ready…to increase them.[41]

At the time of this October 2002 interview, al Qaeda had claimed responsibility for an attack that same month against a French oil tanker and for the attack against German tourists at a Jewish synagogue in Tunisia the previous March. This method of communication serves two purposes: it boosts the morale of al Qaeda operatives who can no longer regularly meet with bin Laden and al-Zawahiri in Afghanistan, and it conveys the message to al Qaeda's supporters that the organization is still intact and that they are continuing to conduct successful operations. Easily accessible and widely used technologies, such as the Internet, also give terrorists the advantage of spreading the message that they want to send to counteract the often negative press that terrorism receives in the popular media.[42] Al Qaeda and its affiliate organizations have used not only video and audio production to craft the message they want to send to their followers and the broader public, but have also created a number of websites to spread information. [43]

The United States and its allies can exploit the inherent vulnerabilities of these technologies for intelligence gathering, especially as terrorists rely more upon these means, rather than direct face-to-face communications for operational planning.[44] Terrorists compromised in an attempt to circumvent electronic detection are also relying more heavily on trusted couriers to deliver important handwritten messages with information that terrorist leaders must have.[45] Another consequence of al Qaeda's awareness of Western intelligence gathering methods is the deliberate creation of disinformation and noise in the system to confuse and overwhelm intelligence agencies tracking terrorist communications.

Finally, it also appears that the threat from individual terrorists is increasing. A poignant example of this phenomenon is the case of Hesham Mohamed Ali Hadayet, the Egyptian who shot two Israeli agents at the El Al counter at Los Angeles International Airport on July 4, 2002. [46] It is important to note that the threat of individual attacks is not solely from al Qaeda and its affiliates. Individuals acting on their own without any particular group association and likely to sympathize with al Qaeda, the Palestinian cause, or any other grievance against the United States and its policies overseas also pose a threat. While individual terrorists are harder to detect and stop, individuals, particularly those who have very loose ties to terrorist organizations, are often not as well trained and are therefore more likely to fail or compromise their operations. They are also less likely to have the technical expertise to carry out large-scale operations on their own. Of particular concern to the United States are its own citizens who are loyal to, trained by, or

---

[41] Ibid.
[42] Bruce Hoffman, "Underground Voices: Insurgent and Terrorist Communication in the 21st Century," unpublished paper, August 2002.
[43] For example, www.jihad.net, www.mojahedoon.net, www.hizbollah.org, and www.jihad-online.com.
[44] Mike Williams, "Analysis: What next for al Qaeda?" November 22, 2001, http://news.bbc.co.uk/1/hi/world/south_asia/1678467.stm, accessed October 25, 2002.
[45] Peter Finn, "Al Qaeda Deputies Harbored By Iran," *Washington Post Foreign Service*, August 28, 2002, available at www.patriotdrive.com/waronterror/patriot/News/iranharbor.html, p. A01.
[46] "The FBI is investigating the July 4 double murder-suicide at Los Angeles International Airport as possible terrorism even though there's no evidence linking the alleged shooter to any terrorist group, a spokesman said Tuesday." Christopher Newton, "FBI Labels Inquiry Into Los Angeles Airport Shooting a Terrorism Investigation," Associated Press, September 3, 2002, available at http://ap.tbo.com/ap/breaking/MGAGDWGGO5D.html, accessed October 29, 2002.

inspired by al Qaeda, who are willing to act on his behalf both at home and abroad against Americans. It is to these and other threats in the United States that we now turn.

"Homegrown" Threats

Although significant and deserved focus has been directed at the danger posed by foreign terrorists coming from abroad, the panel believes it is important to remember the continued threat posed from domestic sources inside the United States. Globalizing factors have blurred some of the distinctions between strictly domestic versus international terrorism, and yet, the term "domestic terrorism" is still most appropriate in describing some of the threats internal to the United States, as discussed below.[47]

Doubtless the greatest asset to al Qaeda today in striking in the United States would be the activation or recruitment of individuals who are American citizens. Of course, the threat is still significant from foreign elements attempting to infiltrate into the United States or from non-citizen "sleeper" agents who had even been put in place before September 11. U.S. citizens and legal residents, inspired by al Qaeda's ideology, might serve as a support base—or possibly operatives—in future al Qaeda attacks. Arrests this year of terrorist suspects in Detroit, Michigan,[48] in Lackawanna, New York,[49] and in Portland, Oregon[50] are illustrative. The alleged "dirty bomb" plot of Jose Padilla (a.k.a., Abdullah al-Muhajir), an American citizen who apparently sought to carry out attacks against his country also demonstrates the potential threat, despite Padilla's amateurish approach.[51] Similarly, American citizens that support foreign interests other than al Qaeda, such as the Palestinian issue, may present a particularly difficult scenario to defend against because American citizens may not present as recognizable a threat. This is particularly pertinent given the recent "justification" for attacking American citizens by bin Laden.[52] In this statement, the American people are singled out as specifically responsible for the actions of the U.S. government because of the democratic process in the United States, and thus the justification for targeting American citizens for al Qaeda terrorist violence has been specifically broadened.

In the past, Palestinian groups such as Hamas, Hezbollah, and the Palestinian Islamic Jihad (PIJ) have insisted that their attacks were part of a limited struggle against Israel.[53] While these groups have not agreed with U.S. government support for the state of Israel, they have not targeted U.S.

---

[47] The panel is aware of the current debate over the utility of these labels but finds the category helpful in making distinctions between those who might attack from outside the U.S. and those who originate their activities within the United States.

[48] See, BBC World News, June 11, 2002, *Profile: Jose Padilla*, available at, http://news.bbc.co.uk/1/hi/world/americas/2037444.stm

[49] U.S. Arrests Six in Probe of Possible al Qaeda Group, PBS Online News Hour, September 16, 2002, available at, http://www.pbs.org/newshour/updates/qaida_09-16-02.html accessed on December 2, 2002.

[50] See for instance, Daikha Dridi and Chris McGann, Infiltrator links men at Oregon ranch to al Qaeda*, Seattle Post Intelligencer Reports*, Tuesday, July 30, 2002.

[51] Amanda Ripley, *Time*, June 16, 2002, "The Case of the Dirty Bomber: How a Chicago street gangster allegedly became a soldier for Osama bin Laden," available at, http://www.time.com/time/nation/article/0,8599,262917,00.html accessed on December 2, 2002.

[52] See, Observer Worldview, November 24, 2002, Translation of bin Laden's Statement, available at, http://www.observer.co.uk/worldview/story/0,11581,845725,00.html.

[53] See for instance, Anders Strindberg, "Interview: 'Imad al-'Almi, Hamas Chief Representative in Syria," *Janes Intelligence Review*, Vol. 13, #12, December 2001, p.56.

citizens inside America.[54] In addition, as noted above, some individuals in these groups have called for a broadening of their strategy to include Americans. If bin Laden's "justification" were to be adopted by Palestinian Islamic groups, the likelihood of increased terrorist activity in the U.S. would be quite significant. Acknowledging this possibility, the government would be prudent to recognize that a ready-made support system for anti-Israeli activism potentially exists in the United States in the form of some "Identity Theology" adherents.[55]

The events of September 11 profoundly affected the worldview of many extremist groups within the United States. Many of these groups, such as the now dispersed Aryan Nations of Idaho and various Ku Klux Klan factions, have struggled to interpret the events in light of their Manichean[56] framework and anti U.S government rhetoric. Some of these groups, particularly the militias, neo-constitutionalists, and others focusing on Second Amendment rights, became for a time, less hostile toward the government following the attacks of September 11.[57] Factions within the militia movement have moved away from talking about wanting to carry out actions against the U.S. government since September 11 and are more inclined to see "foreign terrorists"—even those on their own soil—as the enemy.[58] On the other hand, some adherents of Identity Theology have seen the event as justifying their apocalyptic message.[59]

The reorganization of the Idaho based Identity/neo-Nazi group, Aryan Nations, following the successful civil suit brought against the organization by Southern Poverty Law Center leader, Morris Dees, has created instability within the radical fringe of Identity believers formerly associated with this group.[60] As with the foreign terrorist groups discussed above, splinter groups can be more extreme, and various factions are currently vying for power in this arena, providing the opportunity for up-and-coming leadership to express commitment to their cause by carrying

---

[54] Certain Palestinian groups, such as Hezbollah, have targeted U.S. citizens outside of the United States, as in the 1983 attack on the Marine barracks in Lebanon. The panel is aware that there have been limited fundraising attempts in the U.S. on the part of some of these groups and that Hamas and Hezbollah are know to have cells in the United States. See for instance, James A. Damasak, "Cigarette Smuggling: Financing Terrorism?," *Mackinac Center for Public Policy*, July 9, 2002, available at, http://www.mackinac.org/4461.

[55] Identity Theology is a dynamically evolving theological system based on the British Israel thought—the idea that the British and other Europeans are the "lost tribes of Israel," rather than modern Jewish people. There are four distinct types of Identity theology, three of which pose a terrorist threat. Identity is the theological basis for groups such as Aryan Nations, Covenant, Sword, and the Arm (CSA) of the Lord, and many segments of the Ku Klux Klan, (KKK). For a discussion of the different types of Identity theology see, David W. Brannan, "The Evolution of the Church of Israel: Dangerous Mutations," *Terrorism and Political Violence*, Vol.11, #3, Autumn 1999, pp.106-118, Jeffrey Kaplan, The Context of American Millenarian Revolutionary Theology: The Case of the 'Identity Christian' Church of Israel. Terrorism and Political Violence, Vol. 5, Spring 1993, #1, or, Michael Barkun, *Religion and the Racist Right: The Origins of the Christian Identity Movement.* (Chapel Hill, NC: The University of North Carolina Press, 1997).

[56] Manichean worldviews are a form of Dualism and see every earthly act and situation as a struggle between good and evil. When a terrorist groups is said to hold a Manichean world view, they are distinguished by their perception that the group's view is accepted as "truth" or "good" while all other views are seen as "false" or "evil" and thus directly opposed to the group's worldview.

[57] Based on interviews and informal discussions with various followers of these extremist groups from October 2001—October 2002.

[58] Statement of several unidentified militia activists, December, 2001, Springfield, MO.

[59] From a phone interview with Richard Butler, November 29, 2002.

[60] August Kreis attempted an internal coup and was ousted from the Idaho based group. Kreis has set up a rival faction in Leola, PA. Information on the rival Aryan Nations groups can be found at, http://www.Aryan-nations.org, or see, http://www.twelvearyannations.com/ for Butler's view of the conflict going on within Aryan Nations.

out increasingly violent attacks potentially against individual or government targets.[61] Similarly, the death of National Alliance leader, William Pierce (1933-2002)—author of the influential and radical racialist book, *The Turner Diaries,* which inspired Timothy McVeigh—has left a power vacuum that may lead to increased violence from the white nationalist movement.[62]A more desirable option—that the group might lose direction and synergy following Pierce's death—is also possible.

Anti-globalists continue to be a threat in the United States.[63] This hard to define collection of ideologies is a loose network rather than the traditionally defined cell structure. The violence they promote is often difficult to defend against as it may erupt during a legal protest by American citizens.[64] The loose confederacy created is comprised of coalitions between socialists, environmentalists and anarchists.[65] Earth First—the radical environmentalist group founded by David Broder—has been particularly active collaborating with anti-globalists. Similar concerns emanate from other environmentalist special interest groups such as the Animal Liberation Front, (ALF) and the Earth Liberation Front, (ELF), who have committed over 600 criminal acts in the United States since 1996, resulting in damages in excess of 43 million dollars.[66]

In relation to the panel's primary focus, that of countering the terrorist use of so-called "weapons of mass destruction," the lack of strong centralized command and control has impaired many purely domestic groups from acquiring significant CBRN capabilities. But as the anthrax attacks in fall 2001 showed, even small scale attacks, in terms of casualties, can have a significant impact on the economy and public perception.[67] This does not mean that significant attacks will not come from radical domestic groups; rather, that it will be more difficult to detect an impending attack because it will likely emanate from individuals influenced by certain ideologies rather than coming from a "terrorist organization" *per se*. Timothy McVeigh exemplifies this threat. While not acting completely alone, he was also not part of an identified terrorist organization in the United States, yet he carried out the second largest terrorist attack on American soil.

We now turn to a specific look at the effect of the events since 1999 with regard to the CBRN threat.

---

[61] The increased violence of groups that splinter from the parent groups has been seen in several venues, such as the Real IRA's separation from the PIRA or the PFLP-GC's separation from the PFLP.
[62] While Erich J. Gliebe has been appointed the new leadership of the National Alliance, there have been suggestions that long serving second-in-command, Billy Roper might split from the National Alliance to form his own group.
[63] "Anti-Globalists" emerged as a label, following the 1999, "Battle for Seattle," the violent confrontation between anarchists, their supporters and police at the World Trade Organization (WTO) Summit in Seattle Washington.
[64] As in the case of the WTO Summit in Seattle, see for instance, WTO protests awaken 60's style activism," CNN.com, December 2, 1999, available at, http://www.cnn.com/1999/US/12/02/wto.protest.perspective/ accessed on December 9, 2002.
[65] See a description of the network, Cindy Hasz, "Anarchists of Seattle are Headed to Washington," The American Reporter, Vol. 6, No. 1288, March 15, 2000.
[66] "Inside the FBI: eco-terrorism," *WashingtonPost.com,* February 27, 2002, available at, http://discuss.washingtonpost.com/wp-srv/zforum/02/fbi0227.htm accessed on December 9, 2002.
[67] See for instance, Bruce Hoffman, *Lessons of 9/11* (Santa Monica: RAND, 2002) p. 24 or *American Anthrax Outbreak* of 2001, available at, http://www.ph.ucla.edu/epi/bioter/detect/antdetect_intro.html,

The Threat of Unconventional Weapons

It continues to be surprising that the potential power of unconventional weapons remains largely untapped by terrorists. As the panel concluded in 1999, "the hurdles faced by terrorists seeking to develop true weapons of mass . . . destruction are more formidable than is often imagined."[68] That conclusion is equally valid in 2002. As a U.S. General Accounting Office official testified to Congress last year, technical and operational challenges remain formidable obstacles to terrorist acquisition and use of unconventional weapons.[69] The observation made by the authors of *America's Achilles' Heel* four years ago remain valid: "A combination of motivational constraints and technological barriers explains why the thresholds to acquisition and use of NBC [nuclear, biological, chemical] weapons by non-state actors have almost never been crossed."[70]

Bin Laden has been quoted as saying that the procurement of unconventional weapons is a "religious duty."[71] But even al Qaeda, with its vast resources, global network of operators, and shadow businesses has so far seemed incapable of developing or acquiring a sophisticated chemical or biological weapons capability, although they have demonstrated an interest in doing so.

Although terrorists may be able to overcome technical and operational hurdles in the future, particularly if they receive assistance from states, they have historically employed explosives and firearms, which are easier to produce and use than unconventional weapons. The al Qaeda terrorists who killed nearly 3,000 at the World Trade Center did so using comparatively simple means—commercial passenger aircraft laden with jet fuel. They did not employ CBRN weapons, as many U.S. government officials feared al Qaeda might.

In this discussion, though, it is critical to separate intentions from capabilities. For a full discussion on the difficulties of obtaining and using chemical, biological (including against agricultural targets), radiological, and nuclear weapons, we direct you to the first panel report. The challenges outlined in that initial examination in developing or acquiring these weapons were reinforced by many of the events over the past three years. Changes in the appreciation of the threat from unconventional weapons with respect to major events related to terrorism are discussed below.

The Implications of September 11 and Other Recent Events for the Use of CBRN Weapons

September 11, 2001: Three aspects of the September 11 attacks have important implications for the possible terrorist use of CBRN weapons in the future. First, terrorists willing to destroy skyscrapers filled with people will probably not hesitate to use unconventional means to cause similarly high numbers of casualties if the groups were able to overcome the technical and

---

[68] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [Gilmore Commission], *First Annual Report to the President and the Congress*, vol. I, *Assessing the Threat* (Washington, DC: RAND, December 15, 1999), p. 20.

[69] Henry L. Hinton, testimony before the U.S. Senate Committee on Governmental Affairs, October 17, 2001, GAO-02-162T, p. 4.

[70] Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear Biological, and Chemical Terrorism and Covert Attack*, (Cambridge, Massachusetts: MIT Press, 1998), p. 28.

[71] John J. Lumpkin, "Bin Laden sees 'religious duty' in targeting all Americans," *The Associated Press*, September 28, 2001, http://www.oakridger.com/stories/092801/stt_0110040004.html, accessed December 6, 2002.

operational hurdles. Second, historically, terrorists who have sought to use unconventional weapons have failed to inflict the number of casualties these weapons could potentially cause because of a combination of their inflated expectations about their capabilities and the amateurishness of their effort.[72] The September 11 attackers demonstrated patience, determination, and practicality that may enable their confederates to succeed in some future spectacular use of unconventional weapons where other groups have only been able to muster an amateurish level of attack. The motivations and determination of al Qaeda should not necessarily be interpreted as indicators of an inevitable escalation to using CBRN weapons. However, these aspects of the September 11 attack and the evidence discovered in Afghanistan of considerable interest in unconventional weapons bears attention. Finally, the September 11 attacks demonstrated that even al Qaeda, a terrorist organization with significant resources, both human and financial, chose to use a "conventional" weapon albeit with innovative *tactics* (fully-fueled airliners) to strike a symbolic target and kill a large number of people rather than using CBRN weapons. Al Qaeda has demonstrated that it can have mass effects—a significant disruption of society, huge economic losses, strong reactions by governments—without the necessity of using an unconventional weapon—a so-called "weapon of mass destruction." Al Qaeda achieved "mass destruction," by anyone's logical definition, in September 2001.

Discoveries in Afghanistan: Many al Qaeda safehouses in Afghanistan contained documents the terrorists had collected from the Internet on nuclear, biological, and chemical weapons. Director of Central Intelligence (DCI) George Tenet told Congress that al Qaeda "was working to acquire some of the most dangerous chemical agents and toxins."[73] He also testified that "[d]ocuments recovered from al Qaeda facilities in Afghanistan show that bin Laden was pursuing a sophisticated biological weapons research program."[74] The DCI further stated that al Qaeda provided training in Afghan camps "in the production and use of toxic chemicals and biological toxins."[75] Department of Defense officials had also indicated that evidence of al Qaeda's efforts to acquire biological weapons (BW) was discovered, although they judged the capability as rudimentary.[76]

The interest in acquiring a capability and actually using it are quite different propositions. Although Tenet categorized al Qaeda's efforts as "sophisticated," several U.S. officials have noted that the evidence discovered by American forces showed al Qaeda's great interest in unconventional weapons, but little evidence of much success in acquiring the capabilities to use them. U.S. Secretary of Defense Donald Rumsfeld, has repeatedly stated that while there is evidence of considerable al Qaeda interest in unconventional weapons, nothing thus far suggests

[72] See, Bruce Hoffman, Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations," RAND, P-8039, 1999, p. 34; and ; Jonathan B. Tucker, Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons, (Cambridge, Massachusetts: MIT Press, 2000), pp. 256-257.
[73] Testimony of Director of Central Intelligence, George J. Tenet, Worldwide Threat--Converging Dangers in a Post 9/11 World, Senate Select Committee on Intelligence, February 6, 2002, available at http://cia.gov/cia/public_affiars/speeches/dci_speech_02062002.htm, accessed December 5, 2002.
[74] Testimony of George J. Tenet, Director of Central Intelligence, before the U.S. Senate Armed Services Committee, March 19, 2002.
[75] Written Statement for the Record of the Director of Central Intelligence, Joint Inquiry Committee, October 17, 2002, available at http://www.cia.gov/cia/public_affairs/speeches/dci_testimony_10172002.html accessed on December 5, 2002.
[76] Judith Miller, "Lab Suggests Qaeda Planned to Build Arms, Official Say, *New York Times*, September 15, 2002.

that the terrorists have been able to acquire or weaponize CBRN. [77] Even DCI Tenet's testimony reveals this distinction. He stated that the evidence proved only that they were "working to acquire" chemical agents and that they were "pursuing" a biological weapons capability—*not* that al Qaeda had been successful in either obtaining or fabricating on their own such weapons.

The CNN tapes of an al-Qaeda member killing a small dog with a toxic liquid provided gruesome confirmation of a crude capability to use toxic chemicals to kill.[78] This film footage—showing the agonizing death of a dog—confirms what Ahmed Ressam revealed in court testimony: in al-Qaeda training camps, trainers demonstrated how to use a toxic chemical, probably potassium cyanide, to kill small animals. Ressam testified that he was also instructed on how to introduce toxic chemicals into the air intake vent of a building.[79] While film footage and Ressam's testimony are disturbing, they reveal only a primitive capability to use toxic chemicals as a means of killing. Ressam's testimony about training with chemical agents in 1998[80] is consistent with discoveries made in Afghanistan in 2001 and 2002. This suggests, from available evidence, that al-Qaeda's chemical weapons capabilities remain unsophisticated.

If these efforts are indicative of the sophistication of al Qaeda's capability to use unconventional weapons, they are hardly different from previous attempts by terrorists to use these types of weapons. While the group has demonstrated interest in acquiring and using chemical, biological and nuclear weapons, our fears exceed what they seem capable of accomplishing *at this time*. Further, if a so well-funded and well-resourced an entity as al Qaeda has difficulty in building or acquiring significant unconventional weapons capabilities when they have both the motivation to kill as many Americans as possible and the resources to organize large-scale attacks, then it is unlikely that other less sophisticated or well-resourced groups, or those with less ambitious agendas, will be able, in the near future, to acquire or build a CBRN weapon that could kill people in large numbers without detection. Nevertheless, as we state elsewhere, terrorists may still attempt to use weapons, including CBR (but probably not N), with the intent of achieving "mass effect" but are unlikely to achieve "mass casualties" or "mass destruction." The danger, however, remains, that any nonstate adversary might acquire more sophisticated CBRN capabilities from the arsenals of established nation-states.

Anthrax attacks: The anthrax attacks last autumn represent another new development that must be taken into account as part of an assessment of the overall CBRN threat. While the attacks tragically killed five people and 17 others contracted the disease, these attacks caused far fewer casualties than the September 11 attacks, the African embassy bombings in 1998, the 1995 Oklahoma City bombing, or the 1993 World Trade Center bombing. Despite the significantly lower number of casualties, the anthrax attacks caused considerable public concern, but no real panic. Nevertheless, the government response in the aftermath of those attacks is another

[77] Transcript of testimony by Secretary of Defense Donald H. Rumsfeld, Defense Subcommittee of the Senate Appropriations Committee, May 21, 2002, available atwww.defenselink.mil/speeches/2002/s20020521-secdef.html accessed December 6, 2002. See also, Transcript of DoD News Briefing featuring Secretary Rumsfeld and General Richard Myers, January 16, 2002.
[78] Dana Priest, "Archive of Al Qaeda Videotapes Broadcast, Dogs Shown Dying from Toxic Vapor, *Washington Post*, August 21, 2002, p. A13.
[79] Testimony of Ahmed Ressam, Prosecution Witness, *United States of America v. Mokhtar Haouri*, S400Cr.15(JFK), June 3, 2001, pp. 620-622.
[80] Ibid, p. 546.

example of the need for a more comprehensive understanding of such threats, better planning, and more effective communications.

Regardless of the perpetrator of the attacks (who at this writing is still unknown), the sophisticated nature of the material and its potency marks a watershed.[81] Experts previously believed that a state weapons program could only produce this type of material. Similarly, most experts assumed that a state would not clandestinely attack for fear of retaliation. [82] If the attacks are the work of a state or a state using a terrorist group to conduct the attacks, this is a new development.

If the attacks are the work of an individual, then this again points to the difficulty in tracking down and stopping a committed lone terrorist. A consensus is emerging in the U.S. government and among outside experts that the perpetrator or perpetrators had some connection to the U.S. biodefense program.[83] Those involved would be most likely to have the capability to produce such a weapon. If the perpetrator or perpetrators of the anthrax attacks are in fact "our own," it raises fundamental issues about security at our Federal laboratories, personnel background screening, and the nature and scope of our defensive program. Alternatively, if the perpetrator is indeed a foreign state waging a covert attack against the United States, this is also a significant development. This case remains an important consideration in any threat assessment, although until the perpetrator is identified, it is difficult to know how to characterize the implications for the threat of the future use of biological weapons. Despite the tragic loss of life caused by the event, useful insight has been gained into the requirement to improve the capabilities of law enforcement authorities and public health officials to handle such an attack.

The Arrest of Jose Padilla: The threat of a radioactive dispersal device, or dirty bomb, was highlighted by the detention of Jose Padilla, an al Qaeda member who allegedly plotted to develop such a device in the United States to cause panic, death, and destruction. Despite initial indications to the contrary,[84] FBI officials now believe that the plot was never fully developed, and that Padilla was not a well-trained operative.[85] Although the Padilla plot did not have much substance, there are insufficient controls on access to radioactive material in the United States; this material may pose a threat in the future if acquired by people with nefarious objectives. In

---

[81] Richard O. Spertzel, testimony before the House Committee on International Relations, "Russia, Iraq, and Other Potential Sources of Anthrax, Smallpox, and Other Bioterrorist Weapons," December 5, 2001, available at www.house.gov/international_relations/sper1205.htm accessed December 6, 2002.

[82] Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear Biological, and Chemical Terrorism and Covert Attack* (Cambridge, Massachusetts: MIT Press, 1998), pp. 28 and 94. See also, Brad Roberts and Michael Moodie, "Biological Weapons: Toward a Threat Reduction Strategy, *Defense Horizons*, No. 15 (Center for Technology and National Security Policy, National Defense University), July 2002.

[83] Barbara Hatch Rosenberg, "Anthrax Attacks Pushed Open an Ominous Door," *Los Angeles Times*, September 22, 2002. See also, Nicholas D. Kristof, "Anthrax? The F.B.I. Yawns," *New York Times*, July 2, 2002, p. 21; Laura Rozen, "Our Own Worst Enemy?" *The American Prospect*, Vol. 13, Issue 9, May 20, 2002, available ar http://www.prospect.org/V13/9/rozen-1.html accessed April 24,2002; Andrew Stephen, "America," *New Statesman*, August 5, 2002.

[84] "Transcript of the Attorney General John Ashcroft Regarding the transfer of Abdullah Al Muhajir (Born Jose Padilla) to the Department of Defense as an Enemy Combatant," June 10, 2002 available at http://www.justice.gov/ag/speeches/2002/061002agtranscripts.htm on December 5, 2002.

[85] Mark Hosenball, Michael Hirsh and Ron Moreau, "Odyssey Into The Shadows," *Newsweek*, June 24, 2002. Kevin Johnson and Toni Locy, "Threat Of 'Dirty Bomb' Softened," *USA Today,* June 12, 2002.

addition, U.S. officials have indicated that low-grade uranium-238 was discovered in tunnels in Afghanistan near a former al Qaeda base, enough to make one "dirty bomb."[86]

Use of Toxic Material as Weapons and Threats Against Industrial Facilities: In addition to more traditional chemical weapons, terrorists have shown an increased interest in employing toxic industrial chemicals, pesticides, and commercial poisons. The al Qaeda attack in Tunisia in which a gas truck was used as a weapon against a synagogue and the thwarted attack on a main gas storage facility in Israel may be a harbinger of attacks to come in the short- to mid-term.[87] There is a potential for an attack using industrial materials that can be as toxic as military grade weapons. An attack on a facility storing or manufacturing toxic materials could also produce substantial effects, potentially including mass casualties.[88] Security measures protecting these materials and controls on hauling them around the country continue to be weak and may not thwart the efforts of determined terrorists bent on using poison as a weapon.[89] The use of toxic materials by terrorists again represents a case where the United States has recognized a huge potential vulnerability, but where a clear threat from terrorists has not been demonstrated.

The Outbreak of Foot and Mouth Disease in the UK and the Threat to Agriculture: There have been no significant attacks on agriculture since the panel's first report; however, the outbreak of Foot and Mouth Disease (FMD) in the UK in 2001 highlighted the potential economic consequences of a large-scale agricultural attack. This combined with the trend towards attacking economic targets noted above enhances the chance that America's agriculture base may become a target.

The agricultural sector has still not received the focus that other infrastructures have received with regard to effectively developing vulnerability-threat analyses used to maximize both anti-terrorist contingencies and consequence management modalities. Agriculture and the general food industry remain critical to the social, economic and, arguably, political stability of the United States, yet there are significant vulnerabilities within the agricultural sector.[90] What makes the vulnerabilities inherent in agriculture so worrying is that the capability requirements for exploiting these weaknesses are not significant and certainly far less that than those needed for a biological attack against humans. Notwithstanding its operational ease relative to other unconventional attacks, the ramifications of a concerted bio-assault on the U.S. meat and food base would be far-reaching and could easily extend beyond the immediate agricultural community to affect other segments of society.

Despite the relative ease by which an act of agroterrorism could be carried out and the severe ramifications that a successful assault could elicit, it has not appeared as a primary form of terrorist aggression. Traditionally, terrorist tactics have been designed to produce immediate, visible effects. In this light, it is perhaps understandable that biological attacks against agriculture have not yet emerged as more of a problem. Since 1912, there have been twelve documented cases involving the substate use of pathogenic agents to infect livestock or contaminate a related produce. Several could be termed terrorist in nature: the 1984 Rajneeshee

[86] Neil Doyle, "Al Qaeda Nukes Are Reality, Intelligence Says," *Washington Times*, October 28, 2002, p. 17.
[87] John Kifner, "Israel Thwarts Bomb Attack, but Fears More to Come," *New York Times*, May 25, 2002, p. 3.
[88] See http://ifpafletchercambridge.info/transcripts/dallas.htm.
[89] Andrew C. Revkin, "Little Done Yet to Keep Trucks from Terrorists, *New York Times*, October 20, 2002, p. 1
[90] Ellen Shell, "Could Mad Cow Disease Happen Here?" *The Atlantic Monthly* 282/3 (1998): 92; "Stockgrowers Warned of Terrorism Threat," *The Chieftain*, August 19, 1999.

salmonella food poisoning in Oregon; the 1952 Mau Mau plant toxin incident in Kenya;[91] the Palestinian plot to poison Israeli oranges; and the Chilean grape scare.[92] That being said, agroterrorism could well emerge as a favored form of secondary aggression designed to exacerbate the general societal disorientation caused by a more conventional campaign of bombings. The mere ability to employ cheap and unsophisticated means to undermine a state's economic base and possibly overwhelm its public management resources potentially give livestock and food-related attacks a highly attractive, cost-to-benefit payoff that would be of considerable interest to any group faced with significant power asymmetries. These considerations have particular pertinence to an organization, such as al Qaeda, which has repeatedly stated its intention to conduct economic warfare against the United States and explicitly endorsed the acquisition and use of biological agents to undermine American interests.[93] Though economic warfare has been threatened by al Qaeda, there has been no clear indication that they or other terrorists are currently interested in attacking agriculture on a large scale. Nevertheless, several factors, including our continuing success at forcing terrorists to change tactics and targets, could in the future cause them to consider this avenue of attack.[94]

The Impact of State Assistance to Terrorist Groups on CBRN Acquisition

Terrorists might overcome some of the technical and operational barriers to weaponizing chemical, biological, and nuclear materials with assistance from a state's unconventional weapons program. Such assistance would be particularly important in the case of nuclear weapons. Obtaining such a weapon, or acquiring the fissile material required to build a crude nuclear device, remains arguably the most formidable hurdle for terrorists.[95] Even states have struggled to marshal the resources necessary to meet the technical and operational challenges, and the states that have acquired these capabilities are not known to have transferred the capability to terrorist groups.

However, the normative prohibition against states transferring CBRN weapons capability to terrorists may be eroding. President Bush has repeatedly indicated his concern over states that clandestinely seek nuclear, biological, and chemical weapons in contravention of a number of

[91] The group used the African Milk Bush to poison 32 steer at a Kenyan mission. "W. Seth Carus, "Bioterrorism and Biocrimes: Illicit Use of Biological Agents in the 20th Century," Center for Counterproliferation Research, National Defense University, July 1999 revision, and Pushpraj Singh, "All About Agricultural Terrorism," November 15, 2001.

[92] In the former, between 1977 and 1979, over 40 percent of the Israeli European citrus market was curtailed by a Palestinian plot to inject Jaffa oranges with mercury. The latter was a plot in 1989 by anti-Pinochet extremists to lace fruit bound for the U.S. with sodium cyanide. Import suspensions subsequently imposed by the U.S., Canada, Denmark, Germany and Hong Kong cost Chile in excess of US$200 million in lost revenue earnings. See Ron Purver, *Chemical and Biological Terrorism: A New Threat to Public Safety*, Conflict Studies No. 295 (London: Research Institute for the Study of Conflict and Terrorism, 1996/1997), pp. 13-14; David Rapoport, "Terrorists and Weapons of the Apocalypse," paper presented before the "Future Developments in Terrorism" Conference, Cork, Ireland, March 1999, pp. 13-14; and "Plant Scientists Sound the Alarm on Agroterrorism," *The Philadelphia Inquirer*, September 13, 1999.

[93] "The World's Newest Fear: Germ Warfare," *The Vancouver Sun* (Canada), September 24, 2001; "Fear and Breathing," *The Economist*, September 29, 2001, p. 37.

[94] See Chapter VII, and Appendices E and F.

[95] Central Intelligence Agency, questions for the record from the Worldwide Threat Hearing before the Senate Select Committee on Intelligence, April 8, 2002, p. 7, available at http://www.fas.org/irp/congress/2002_hr/020602cia.html.

international agreements[96] and also that provide extensive support to terrorist groups.[97] In a similar vein, Secretary of Defense Rumsfeld testified that, "we have to recognize that terrorist networks have relationships with terrorist states that have weapons of mass destruction and that they inevitably are going to get their hands on them."[98] During the Cold War, the Soviet Union and China supported a number of terrorist groups and insurgency movements that used terrorism as a tactic. The countries provided conventional arms, sanctuary, financing, intelligence, documentation, and logistics. Today, the states that are of greatest concern with respect to CBRN terrorism are Syria, Iran, and Iraq. All of these countries seek unconventional weapons capabilities or already possess them and have contacts with terrorist groups.[99] This danger is not inevitable, but neither can it be dismissed. Statements by the President and other officials may be "brightening" the red line of deterrence.

Among states that sponsor terrorism, Iran is the most active. Iran provides a full range of support to Lebanese Hezbollah and to a somewhat lesser extent Hamas, Palestinian Islamic Jihad, and military entities affiliated with the Palestinian Authority. While these terrorist groups have not traditionally attacked targets on U.S. soil, as noted above, at least some individuals within these groups are advocating broadening their objectives to global targets. In addition, Iran provides at least transit and temporary safe haven to some al Qaeda members and their associates. Groups supported by Iran were purportedly responsible for the devastating attack on U.S. interests at Khobar Towers in Saudi Arabia. The FBI argued in court documents that elements of the Iranian government were involved in the 1996 attack, which killed 19 U.S. service people and injured many more.[100] The case of Khobar Towers is a good example of how a faction within the Iranian government might have provided an unconventional capability to a terrorist group. This becomes more problematic if the faction within the government that controls part of the state's unconventional weapons program provides unauthorized assistance to a terrorist group they sponsor.

After Iran, Syria is the most active state sponsor of terrorism and is included on the U.S. State Department list of state sponsors of terrorism. Libya is another country that has a history of supporting terrorism and is known to possess chemical weapons.

Iraq provides sanctuary to a number of notorious anti-Israeli Arab nationalist groups, but it is not nearly as active in its support as either Iran or Syria. Senior U.S. officials have stated that Iraq trained terrorists on how to handle chemical weapons.[101] Some Iraqi defectors alleged that Iraq trained terrorists in the use of chemical and biological weapons.[102] Iraq's defeat in the Gulf War and repeated American military attacks in the years following the war undoubtedly have boosted Iraqi dictator Saddam Hussein's intense hatred of the United States. Yet, despite Hussein's

---

[96] Including the Nuclear Non-Proliferation Treaty, the Chemical Weapons Convention and the Biological Weapons Convention.
[97] Office of the Press Secretary, "President Delivers State of Union Address," January 29, 2002, [http://www.whitehouse.gov/news/releases/2002/01/20020129/11.htm.]
[98] Transcript of testimony by Secretary of Defense Donald H. Rumsfeld, Defense Subcommittee of U.S. Senate Appropriations Committee, May 21, 2002.
[99] U.S. Department of State, *Patterns of Global Terrorism* (2001), available at http://www.state.gov/s/ct/ris/pgttpt/2001/htl/10249.htm accessed on December 6, 2002.
[100] Elsa Walsh, "Louis Freeh's Last Case," *The New Yorker*, May 14, 2001, pp. 68-79.
[101] Interview with Dr. Condoleeza Rice, National Security Advisor, The News Hour, September 25, 2002.
[102] Gwynne Roberts, "Militia Defector Claims Baghdad Trained Al Qaeda Fighters in Chemical Warfare," *London Sunday Times*, July 14, 2002, p. 23.

motivation to use terrorist forces as a vector against the United States and the possibility that Iraq could transfer unconventional weapons capabilities to terrorist groups for their own purposes, there is no consensus that this has occurred.

Given the weapons ambitions of these states and their contacts with terrorist groups, the possibility of transfer of CBRN weapons between these states and terrorist organizations requires careful attention. While the danger remains that the context may change and these states will view transfers of unconventional weapons to terrorist groups as in their interest, there is no evidence that they have yet done so. The United States should work to maintain this prohibition.

Unauthorized assistance by weapons scientists from some of the newly independent republics of the former Soviet Union may also enable terrorists to develop an unconventional capability on their own. There are reports, for example, of Russian biological weapons scientists helping Iran.[103] While these reports are disturbing, the contact is believed to have been limited in scope and was discontinued after American officials brought the contacts to the attention of Russian scientific officials.[104] Over the decade since the collapse of the Soviet Union, Russia has experienced severe economic troubles. While some nuclear smuggling and brain drain has occurred, it is difficult to "know the extent or magnitude" of these developments, much less to assess their actual implications on both rogue state and nonstate acquisition efforts. [105] Al Qaeda's attempts to cultivate its own expertise in CBRN manufacturing and deployment, however, indicates that the threat of proliferation of Soviet expertise in this area may have been overblown. The potential danger remains, but it should be viewed in the context of the last ten years, during which a multitude of cooperative threat reduction programs have thus far thwarted this danger and managed the threat alongside the improvement of conditions in several of the former republics of the former Soviet Union, most notably Russia. The threat has not materialized, as many officials and analysts feared a decade ago; but continued vigilance is required.

Conclusion

The anthrax attacks of 2001 have continued to keep much of the U.S. focused on the potential for terrorists to employ unconventional weapons. However, our analysis of the threat indicates that terrorists intent on conducting future mass casualty attacks are more likely to use conventional than sophisticated CBRN weapons in the near term. September 11 illustrated that terrorists can achieve a high number of casualties and widespread panic without the difficulties involved in a sophisticated CBRN attack. Furthermore, the few deaths resulting from the anthrax attacks carried out in the United States in the fall of 2001 reinforced the idea that conventional attacks at this stage are likely to produce a larger number of casualties. Outside of al Qaeda and some of its affiliate groups, such as the Egyptian Islamic Jihad, that have acquired at least a crude CBRN capability, only a limited number of groups have access to this material and are capable of

[103] Judith Miller, Stephen Engelberg, William Broad, *Germs: Biological Weapons and America's Secret War* (New York: Simon & Schuster, 2001), pp. 205-207.
[104] Ibid.
[105] National Intelligence Council, Annual Report to Congress on the Safety and Security of Russian Nuclear Facilities and Military Forces, February 2002, available at http?//www.ciagov/nic/pubs/other_icarussiansecurity.htm accessed December 6, 2002. See also, Emily S. Ewell, "NIS Smuggling since 1995: A Lull in Significant Cases?," *The Nonproliferation Review*, Spring-Summer 1998, Vol. 5, No. 3, pp. 119-125.

conducting attacks of this type inside the United States.[106] As a result, fundamental analysis of the first report of the panel remains valid today, albeit colored by some the trends noted above, especially toward increasing lethality.

A better understanding of why terrorists do or do not opt for unconventional weapons may provide direction for strengthening policy measures that will continue to deter terrorist use of these weapons. The "worst-case" scenario approach that has dominated certain U.S. planning and preparedness has resulted in several decisions that may have been made differently if other policies were based on a wider range of scenarios.[107]

The current threat of terrorist acquisition and use of chemical, biological, radiological or nuclear weapons to cause "mass casualties" or "mass destruction" remains, on balance, a lower risk than other means terrorists might use to inflict mass casualties. That said, terrorists may choose the use of an unconventional weapon, especially a chemical or biological one, perhaps even a small-scale radiological one, that can still cause "mass effects" in terms or psychological, sociological, or economic damage. Policymakers should continue to plan for increases in the volume and lethality of terrorism and for attacks across the entire spectrum of weapons (including CBRN), tactics, and targets. In addition, with the passage of time, it becomes more likely that terrorists could have access to or the ability to create and then use unconventional weapons with a mass effect.

Significant efforts have been undertaken to deter, detect, interdict, prevent, and develop response capabilities for terrorism in the intervening three years; however, much remains to be done. This is the subject of the remainder of the report.

[106] U.S. General Accounting Office, *Combating Terrorism: Linking Threats to Strategies and Resources*, GPO Access. July 26, 2000, available at http://www.gao.gov/new.items/ns00218t.pdf, accessed October 29, 2002.
[107] See, for example, the argument in Hoffman, "Lessons of 9/11," (pp. 19-20) that planning would benefit from an approach that, in addition to asking the usual questions of "what could or what might happen?," attempts also to inquire "what hasn't happened, or what type of attacks have terrorists only perpetrated rarely?," and then to walk-backward analytically in assessing these potentialities as a way of obtaining a better understanding of the capabilities and resources required by terrorists to carry out a range of nontraditional attacks.

CHAPTER III. APPLYING CROSS-CUTTING THEMES

Each subsequent chapter of this report will address issues in various functional areas. We have identified several cross-cutting themes that may be related to any number of the issues we address. Where they are applicable, we will highlight those themes in each chapter. Here, we explain our rationale for each of those thematic topics.

Protecting Our Civil Liberties

The civil liberties of all U.S. persons have been paramount in all of the panel's deliberations and are always a key consideration in each recommendation that we make. The Constitutional protections that we enjoy are what make our country unique in all the world. No other country has the same degree of protections or takes the pains to ensure their strict enforcement as ours. We have previously quoted our founding fathers as guiding lights for the consideration of these difficult issues. One of the most appropriate:

> They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety. *Benjamin Franklin, 1759.*

We firmly believe that it will not be necessary to "give up essential liberty" to achieve a marked increase in our security. We have previously recognized that 100 percent security will be unattainable if we maintain our uniquely American way of life. Americans understand and accept that. They only ask of their governments that the most effective measures that can be taken within the context of our Constitutional protections be implemented.

At the same time, the vast majority of Americans understand that for every civil right a corresponding obligation exists; for every privilege there is usually some cost. Driver licenses are not a civil right; they are a privilege that require testing and normally proof of age and photographic identification. Airline travel is not a civil right; it is a privilege that subjects us to what, in other contexts, would be considered an unlawful search.

Striking an appropriate balance will always be a challenge, but we are convinced it can be done. Our analysis indicates that all of the legislation enacted in the aftermath of the attacks of last year—the USA PATRIOT Act and several others—are likely to pass Constitutional muster. Our concern continues to be that we pass legislation that addresses remaining security issues in other than crisis times. Responding to the next crisis after it occurs may run the greater risk of impinging upon our important Constitutional protections.

Enhancing State and Local Capabilities

It is our principal legislative mandate to assess Federal programs for their effectiveness for improving the ability of States and localities to respond to terrorist attacks. Our States and communities must have the knowledge and the resources to fulfill their critical roles in the national effort.

We have from the beginning of our deliberations maintained a key set of principles that have guided our deliberations in this regard:

- All terrorist incidents are local or at least will start that way. Effective response and recovery can only be achieved with the recognition that local responders[108] are the first line of defense and through the proper integration of State and Federal assets into existing response networks.
- Building effective and sustainable response and recovery capabilities requires an "all-hazards" approach that integrates planning and response with existing processes.
- To be most effective, plans and programs for combating terrorism should build on existing State and local management structures and command and control mechanisms.
- Capabilities for combating terrorism should be designed to the greatest extent practicable for dual- or multi-purpose applications, for maximum utility and fiscal economies of scale.
- Effective preparedness for combating terrorism—planning, training, exercises, and operational structures—requires a fully integrated network of Federal, State, and local organizations. At the local level, this network includes the traditional "first responders"—law enforcement, fire, and emergency medical services personnel—and also *must* include other State and local agencies, such as public health departments, hospitals and other medical care providers, and offices of emergency management.

For this report, we add another:

- The effectiveness of programs should be based on carefully crafted, well-understood measures of performance. Without such metrics, we will be relegated to determine effectiveness based the amount of money being spent.

For those reasons, we have consistently adhered to the view that all strategy and programs for combating terrorism inside the United States must be approached from the "bottom up"—starting from the viewpoint of the localities and States, not from a Federal, or "top-down" perspective. As a current example, much of the resources to protect critical infrastructures come from State and local governments, yet the flow of information and certain resources is currently a "top-down" approach—Federal to private sector with minimal State and local engagement. States and localities must be intimately involved in these efforts.

During the current report period, we updated the major nationwide survey that we conducted for our Third Report, by returning to the same survey audience of State and local responders to find out what, if anything had changed. The results are telling. Throughout this report, as appropriate, we include analysis from the most recent survey in each of the substantive chapters, and also include a full analysis of the survey results at Appendix D.

[108] As noted in its *First Annual Report*, the panel has chosen to use "local responders"—as opposed to "first responders"—to characterize those persons and entities most likely to be involved in the early stages following a terrorist attack. That characterization includes not only law enforcement, fire services, emergency medical technicians, emergency management personnel, and others who may be required to respond to the "scene" of an incident, but also other medical and public health personnel who may be required to provide their services in the immediate aftermath of an attack.

Improving Intelligence and Information Sharing

Intelligence—its timely collection, thoughtful analysis, and appropriate dissemination—is the key to effective prevention of terrorist attacks. From the inception of our deliberations, we have said that "more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats."[109] While improvements have been made, that statement is still true today.

The creation of the Foreign Terrorist Tracking Task Force and the U.S. Attorneys Antiterrorism Tasks Forces, the expansion of the regional Joint Terrorism Task Forces (JTTF) and the creation of a National JTTF, and the enhancement of other Federal interagency mechanisms are all important steps. What is unclear is how all of those entities will necessarily be coordinated.

We have made several recommendations in previous reports about ways to improve the sharing of intelligence and other information horizontally and vertically among government entities and which now increasingly must include certain entities in the private sector. We make explicit recommendations in this report, especially in the Strategy and Structure chapter, for additional improvements in those processes.

Promoting Strategic Communications

The attacks of 2001 hopefully have taught us important lessons about the ways in which governments talk to the American people about homeland security issues.

Effective communications serve a variety of salutary purposes:

Preparedness: In the period before a terrorist incident, public communications contribute to preparedness by educating the public and the media about the types of events that might occur, how the government would respond to them, and most importantly, steps the public can take to reduce their personal risk to terrorist impacts. In this way, members of the media will develop an understanding of the types of information that will be important during a terrorist event. And members of the public will be educated about the types of actions that will be required, and the resources that will be available for recovery.

Deterrence: Public communications may play a role to deter terrorist plans if they convey the scale of preparedness, capabilities to limit impacts, and reduced levels of vulnerability. Ideally, this element of public communication would coordinate with other deterrent strategies, most importantly implementing appropriate security measures. The deterrent role of public information can occur at all times: as part of preparedness efforts before a terrorist incident, in the communications immediately following an incident, and as part of long term recovery efforts.

Reassurance: In the time immediately following an event, it is most critical that communications contribute to public reassurance and calming. This can be accomplished through a number of ways: by establishing a sense of control and authority over the current situation, by conveying

[109] *First Report,* p. 57.

the scale of emergency management operations, and demonstrating that the government is working to prevent further terrorist attacks.

Conveying key information: Following certain types of events, there will be a need to communicate with the public to limit the scale of the impacts and to speed recovery. This will be especially critical following a chemical or biological events where there will be a need to limit exposures to hazard materials, direct populations toward medical treatment, and limit the spread of disease. To carry out these tasks, it will be critical to have strong coordination between public communication efforts and internal incident management and public health communication systems (e.g., the Health Alert Network).

There are three temporal components of an effective communications strategy:

- Pre-Attack—Those programs to educate the American public, including the media, on the causes and effects of various terrorist attacks. Some have argued that trying to explain to potential for loss of life from unconventional attacks, especially those with biological agents, will cause unnecessary fear among our fellow citizens. We disagree. We trust the common sense and resiliency of the American people to understand and process information on such threats. The challenge will be to "package" that information in ways that will be most effective. The media should be a central part of that educational process. It is essential to build public trust in government and its pronouncements before attacks occur.

- Trans-Attack—Critical communications as an event is unfolding to lessen public panic and mitigate loss of life and injury. National, State, and local leaders must develop processes for determining, based on different scenarios, who will speak on behalf of each level of government and then exercise those plans prior to events occurring. Advance planning and exercises for communications trans-attack are especially critical for bioterrorist incidents.

- Post-Attack—Effective communications in a post-attack environment to restore public confidence, to mitigate further damage, and to facilitate recovery operations. While this area of communications strategy is more mature, based on the nation's experiences with natural disasters, more needs to be done to plan for more effective communications in the aftermath of an attack by terrorists. The government communications following last fall's anthrax attacks demonstrate of why we need improvements.

Additional proposals for improving strategic communications are discussed in considerable detail in Appendix H.

Enhancing Coordination with the Private Sector

National security is no longer solely the purview of the Federal government, as it was during the Cold War. The private sector controls approximately 85 percent of the infrastructure in this country and employs approximately 85 percent of the national workforce. It is also critical to innovations to protect and defend against terrorism. The *National Strategy for Homeland Security* includes as one of its precepts a coordinated government private sector effort to combat terrorism. As defined in the *Strategy*, the Federal government and the DHS are focusing on protecting vulnerabilities of critical infrastructures. This leaves significant gaps in areas where government private coordination and cooperation is essential, including the innate

interdependencies of their functions and the need for businesses to plan to protect the 122 million people they employ.[110] Gaps in these areas will undermine efforts to secure the homeland.

The *Strategy* does not explicitly recognize the dependence of the Federal government on the private sector in responding to a terrorist event. When the national airspace was shut down to commercial traffic following the September 11 attacks, both the government and the private sector were significantly effected by the limited ability to move people and goods.[111] Military planes performed some of the critical transportation functions, but actions were hampered. One intimate example the transportation shutdown hindered the delivery of life-saving products is the case of Jurgen Kansog, a New Jersey resident. On September 11, 2001, he was one of several patients anticipating the arrival of life saving blood stem cells from overseas. He had already undergone exhaustive chemotherapy and radiation treatment and without the stem cells, which only survive for a limited time after donation, he was likely to die. Because no plan was in place that anticipated the shutdown of all air traffic, the National Marrow Donor Program and others had to work quickly to find a way to transport the cells. In the end, they secured "lifeguard status" from the Federal Aviation Administration (FAA) and used a chartered jet to deliver the material.[112]

Understanding the requirements for obtaining "lifeguard status" is one example of how private and public organizations should work together to plan contingencies that explicitly identify critical interdependencies and solutions ahead of time. A second example of the interdependence is the destruction of significant communications nodes at the World Trade Center, which again impaired both government and private sector response functions.[113] If larger sections of the telecommunications infrastructure were impaired or destroyed, the impact would have been even more significant than that felt from the limitations on civilian airliners because the government does not have pervasive backup systems as it does in the case of air transport.[114] The lack of recognition of the critical interdependencies means that such contingencies as the one described above are not explored, well planned for, or exercised.

The *Strategy* also remains silent on the fact that should a terrorist attack occur, it is likely that many people will be at their places of employment and, thus, the inclusion of the private sector in planning for terrorism is critical to ensure the safety of the private workforce. The government already plans for the safety and security of the Federal civilian workforce who numbered nearly 2.7 million (325,000 in the Washington DC Metropolitan area alone[115]) in

---

[110] Available at http://www.bls.gov/opub/rtaw/pdf/intro.pdf accessed December 2, 2002.
[111] Prior to September 11, the National Airspace System, also know as the "NAS," handled 1.9 million passengers, 40,000 tons of cargo, and 60,000 flights through the system daily. Data from Claire D. Rubin and Irmak Renda-Tanali, "Quick Response Report #140," Natural Hazards Research and Applications Information Center, 2001, available at www.colorado.edu\hazaeds\qr\qr140.html, accessed on December 2, 2002.
[112] "A Life Saved Hope in the Face of Tragedy," National Marrow Donor Program, http://www.marrow.org/NEWS/ARTICLES/lifesaved09102002.html .
[113] The attacks resulted in the loss of five phone-switching stations, two electrical substations, 300,000 telephone lines, and 33 miles of cable. It has been estimated that replacing the destroyed subway lines would cost around $3 billion and that utility repairs, including 300,000 telephone lines, one phone switching station, and six miles of electrical cable are estimated to cost $2 billion. Data from report #140.
[114] It is widely reported that 99 percent of government communications is on the publicly switched network, which is owned by the private sector.
[115] "Federal Civilian Workforce Statistics, The Fact Book," 2002 Edition, Owi-02-02, U.S. Office of Management And Budget.

2001.[116] Private sector planning saves lives. For instance, on September 11, 2001, the emergency response plans or the actions of leaders within companies of the businesses occupying the World Trade Center likely contributed to the relatively successful evacuation of thousands of workers from the buildings.[117] After saving lives, companies then turn to restoring their business functions. Many of the WTC firms began operating relatively quickly after the attacks because of emergency planning that began after the 1987 stock market crash and picked up after the 1993 World Trade Center bombing. However, more lives may have been saved and less money lost if the public and private planners had focused on joint preplanning, exercising, and training.

While the *National Strategy* recognizes the need for inclusion of the private sector in the government's anti-terrorism planning, it is short on details, and an analysis of efforts in this area shows that with the exception of health and medical initiatives, the Federal government does not have a history of cooperative, strategic efforts with the private sector for terrorism preparedness and response. Two areas where the Federal government and private sector work together relatively well are noteworthy, purchasing of goods and services through contracts and grants and protection of vulnerabilities in critical infrastructure, but long-term, strategic partnerships are lacking.

This may change with the creation of DHS. In Section 430 of the bill creating the Department of Homeland Security, the Department is given responsibility for "the preparedness of the United States for acts of terrorism, including. . .coordinating preparedness efforts at the Federal level, and working with all State, local, tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support."

States and localities have a longer history of working with the private sector, primarily on the basis of personal relationships. These entities are currently working together in many cases[118] to develop terrorism prevention and response plans.

Examples of specific public private initiatives are discussed in the appropriate chapters.

[116] There are almost 15 million State and local government civilian employees. Table C-5, Statistical Review Of Government In Utah 2000, Data From U.S. Bureau of the Census, Public Employment Series. The Utah Foundation, available at www.Utahfoundation.Org/Stat_Review/Section_C/Uf%20stat%20review%20table%20c5%200101.Pdf accessed December 1, 2002.

[117] More than 430 companies from 28 countries and employing approximately 50,000 people occupied the World Trade Center.

[118] With the exception, noted above, of direct Federal to private sector on certain critical infrastructure issues.

CHAPTER IV. RESOURCING THE NATIONAL EFFORT

In our previous reports, we have discussed in general terms the types, levels, and targets of Federal funding for combating terrorism. Prior to the attacks of 2001, we suggested that the total *amount* of funding was not as important as the necessity to prioritize funding and direct resources to those areas most in need. We reaffirm that prior conclusion.

In the aftermath of the 2001 attacks, Congress appropriated roughly $40 billion in emergency supplemental funds, of which a little less than $11 billion was for domestic or "homeland security" programs[119]—only $240 million of that being specifically allocated directly to States and localities for enhancing preparedness. In the President's budget request for Fiscal Year 2003, $3.5 billion is intended to be provided directly[120] for State and local preparedness.[121] With this massive infusion of additional Federal resources, setting priorities and applying realistic measures of effectiveness are even more important. For more detailed budget information, see Appendix O.

Rationalizing the Process—States Versus Localities

There is a current and pointed debate about the method or methods for moving Federal resources to State and local response agencies—especially those intended for the local level. States and localities are very much at odds over the way in which Federal funds should flow. The stark level of that disagreement was made apparent to this panel in materials provided to us during the course of our deliberations, especially at our meeting in June of this year, when representatives of organizations of State entities on the one hand and local entities on the other pointedly presented their respective positions to us.

Many localities and the response organizations within them argue that such Federal funds, or at least some sizable portion of them, should be channeled directly to the localities, bypassing any measure of State control. The rationale for that argument is that States will "siphon off" too large a share of those resources for applications at the State level and that localities will, therefore, not receive the levels of funding necessary to improve preparedness significantly or that State agencies can delay the timely application of resources.

There is some merit to that argument, based on certain historical precedents in other contexts. Nevertheless, we continue to adhere to the view that Federal funds provided for the purpose of improving local capabilities must be subject to a level of prioritization.[122] The only logical way to do that, in our view, if for States to exercise some degree of oversight over the application of

[119] Approximately $8.2 billion was designated as assistance to Pennsylvania, New York, and Virginia to aid in the immediate mitigation and response activities, and an additional $2.5 billion was made available at to HHS as part of its emergency fund to assist the Federal, State, and local public health system

[120] An additional $1.2 billion has been requested to increase hospitals' capacity to respond to bio-terrorism incidents, and $175 million to improve interoperability in communication networks between Federal, State and local entities.

[121] At the time of the writing of this report, the Congress has passed only two of thirteen regular appropriations bills for Fiscal Year 2003.

[122] See our *Third Report,* at p. 10.

such funds to ensure that resources are allocated on the basis of assessed needs.[123] That view has been correctly, we believe, adopted as the general rule by the current Administration.[124]

We have resisted a "one size fits all" approach to this problem. Indeed, every city of a certain population size does not necessarily have to own a specific set of equipment. That is especially true where a number of municipalities make up a larger metropolitan area. Some municipalities and counties have been smart—even in the absence of definitive Federal guidance—in setting up mechanisms for pooling resources and providing mutual assistance in an emergency.[125] In many cases, those mechanisms have been facilitated by broader State level mutual aid efforts. A designated State agency—most likely its emergency management agency or homeland security agency or coordinator—is logically in a position to understand needs on a statewide basis and, therefore, be able to articulate more effective the requirements and priorities for Federal assistance. Determinations in such areas as standardization and interoperability can more effectively be made at the State level as well. The responsibility for overall preparedness within a State ultimately rests with the Governor.

Furthermore, Federal resources should not be distributed to those localities that happen to have the best grant-writers. With 3,141 counties jurisdiction and more than 600 municipalities with a population over 50,000, the Federal government cannot be expected to prioritize allocations for that many jurisdictions. It can, however, make rationale decisions for the application of Federal dollars based on comprehensive State-by-State assessments of capabilities and requirements.

By the same token, States must be held to some reasonable standard in withholding, at the State level, any portion of funds are intended exclusively or primarily for improving local capabilities. It is logical to us that States should be expected to assist in facilitating responses to terrorist attacks that may exceed local capabilities, either through the provisions of State-level response or by coordinating supporting response capabilities from other jurisdictions within the State that is the target of the attack or from neighboring States under mutual assistance compacts.

As a general rule of thumb, we believe that States should not withhold at the State level more than 25 percent of Federal funds that are exclusively or primarily intended for improving local and/or State response capabilities. For those activities where funding is available for combined State and local efforts, the State's share should be no more proportionally that the level of effort of State entities in such combined efforts. In each case, justification for the allocation of funds should be comprehensive and transparent, and periodic reporting and other audit mechanisms should be used to ensure the appropriate expenditure of Federal resources. States must be required to develop comprehensive strategies, combining both local and State-level capabilities and requirements. Those State strategies must be tied to the imperatives in the *National Strategy* and must be updated on an annual basis.

---

[123] For an excellent discourse on the subject, see Spencer S. Hsu and Lyndsey Layton, "Scattershot Spending in Terror Fight," *Washington Post*, September 10, 2002, page A1.

[124] For a contrary view, see Sen. Hillary Rodham Clinton, "First Things First," *New York Daily News,* November 21, 2002, available at http://www.nydailynews.com/news/ideas_opinions/story/38008p-35892c.html.

[125] We have previously noted the Los Angeles Operational Area entities as models in this regard. They still are.

Establishing Appropriate Burden Sharing

In our Third Report, we listed several guiding principles when considering measures for improving State and local capabilities.[126] Among them:

- *Governments at all levels must share in the costs of domestic preparedness and response, but the Federal government should be prepared to provide resources for the "incremental" or "exceptional" costs of combating terrorism beyond those normally required for public health and safety.*

States and localities clearly have the primary burden of providing resources for the health and safety of its citizens. The response capabilities that will inevitably be brought to bear in the event of a terrorist attack—hopefully only very rarely—are for the most part capabilities that are used daily for other purposes—law enforcement, fire services, public health, emergency medical services, primary and emergency medical care, and emergency management of natural disasters. That is logically—and preferably—the case: response capabilities based on an "all-hazards" approach. But it will be a rare case, indeed, where an act of terrorism will not rise to some level of national importance.

While it is appropriate that States and localities should continue to share a portion of preparedness and response for programs to combat terrorism, we believe that a good general rule for the State share of funding as a condition for receiving Federal assistance should be no more than 25 percent and that, where appropriate, such share may be through "in kind" resources. As we stated earlier with respect to the method of funds for States and localities, justification for the allocation of funds for Federal-State burden shared programs should be comprehensive and transparent, and periodic reporting and other audit mechanisms should be used to ensure the appropriate expenditure of Federal resources.

Ensuring a Central Focus

We continue to suggest that setting priorities and allocating resources according to those priorities is essential to an effective national effort to combat terrorism. The establishment of the new Department of Homeland Security (DHS) will hopefully achieve some measure of more effective priority setting for those agencies that will be part of the new Department. Nevertheless, DHS will not "own" all of the Federal assets, including resources designed for assistance to States and localities. A prime example will continue to be the Department of Health and Human Services.

We recommended in our *Second Report* that a White House office for combating terrorism be given certain budget oversight and controls. We continue to believe that such a function is required for setting resource priorities for Federal programs for combating terrorism, and one that is implemented before the Office of Management and Budget is required to make budget choices among a multitude of other competing priorities. That function can and should be accomplished by the White House Office of Homeland Security.

[126] *Third Report,* pp. 6-7.

We have also previously recommended "consolidating information and application procedures for Federal grant programs for terrorism preparedness in the Office of Homeland Security." With the advent of DHS, it is conceivable that such a function could be performed by that Department, as it will own many such grant programs after full consolidation. In any event, those processes should be consolidated in one central location and with a standard set of forms for grant application, in order to reduce confusion among States and localities regarding the availability of grants and the processes for applying.

Determining "How Much Is Enough"

In our *Third Report,* we recommended "that the Congress increase the level of funding to States and local government for combating terrorism." That is now—appropriately—starting to be accomplished. In our earlier reports and again here, we avoid placing a specific price tag on the costs in Federal funds for improving State and local capabilities. We continue to adhere to the view that the key it is not necessarily the total amount of funds but the necessity to ensure that such resources are applied most effectively. We do not, therefore, apply some arbitrary "scorecard" of how much or how little Federal funds have been provided to enhance State and local efforts from year to year, but rather how effective the application of those funds have been or are likely to be over time. We note again an example that we have discussed previously: the lack of resources for sustaining programs in the out years. Irrespective of the formula that may be applied for burden sharing by States and localities, most Federal programs, especially those for training and equipping State and local responders, must be designed with clear goals and implemented with long-term sustainment in mind.

Measuring Effectiveness

However resources are applied and at whatever level, more must be done to create and implement a system of metrics for judging how well resources are being applied over time. Program evaluations must be more than just an audit trail of dollars and must be part of an integrated metrics system. A program in an agency may impact or duplicate or even contradict the intent of a program in another. It will be incumbent on the White House Office of Homeland Security to ensure a Federal agency-wide approach to such measures.

As we have previously stated, we as a nation can never expect to be 100 percent prepared to deal with every possible terrorist attack scenario. But without a comprehensive approach to measuring how well we are doing with the resources being applied at any point in time, there will be very little prospect for answering the question, "How well prepared *are* we?"

CHAPTER V. ORGANIZING THE NATIONAL EFFORT

ASSESSING THE NATIONAL STRATEGY

The capstone recommendation in our S*econd Report* was the need for a comprehensive, coherent, functional national strategy: "The President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office." In that report, we described, in considerable detail, our proposed framework for that strategy.

In July of this year, the President approved for release the first *National Strategy for Homeland Security*.[127] To lay the groundwork for most of the recommendations in this chapter, we start with a commentary on that *National Strategy* from the panel's perspective, for the most part tracking the subject headings of the chapters on "critical mission areas" in that document.

General Comments

We applaud the President and his staff for publishing this comprehensive vision to see as the framework for the entire national effort. It is a foundation document and an important first step. It should not—indeed it cannot—be seen as being all of the answers to the challenges that we face. It will require periodic updates: we suggest annually. It will require detailed implementation plans; some are already being developed.

It contains well-crafted "vision" statements of where we should be headed as a nation. It acknowledges—as we have said before that any comprehensive strategy must—that there are significant international implications for "domestic" efforts.

It recognizes that this strategic approach must be a truly *national,* not just a Federal approach:

> *. . . .based on the principles of shared responsibility and partnership with the Congress, state and local governments, the private sector, and the American people. The National Strategy for Homeland Security belongs and applies to the Nation as a whole, not just to the President's proposed Department of Homeland Security or the federal government.*[128]

It contains—importantly—definitions of both *homeland security* and *terrorism*:[129]

> *Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.*
>
> *The National Strategy for Homeland Security characterizes terrorism as any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate or coerce civilian populations or governments.*

---

[127] *National Strategy for Homeland Security,* available at http://www.whitehouse.gov/homeland/book/index.html, last accessed December 5, 2002, hereinafter the *"National Strategy."*
[128] *National Strategy*, p. 2.
[129] *Id.*

It contains language about the importance of measures of performance but does not articulate what those measures should be. Importantly, in our view—being consistent with our expressions since our *First Report*—it eliminates the arbitrary, artificial, and confusing distinction between so-called "crisis management" and "consequence management" activities.

It recognizes the importance of creating a national incident management system with an "all-hazards" approach—one that combines preparedness and response for natural disasters, accidents, and intentionally perpetrated attacks.[130]

Definitional Issues

Despite a commendable attempt to reduce confusion by articulating certain definitions, it does not fully accomplish the task. The *National Strategy uses* CBRN or CBRNE[131] and Weapons of Mass Destruction or WMD seemingly interchangeably.

It uses different terms apparently to describe the same function or category: "health," "public health," "medical," "medical care." And it is unclear whether "emergency medical providers" does or does not include emergency medical technicians. It uses other terms interchangeably with not clear delineation or distinction: "anti-terrorism," "counterterrorism," and "combating terrorism." And it is not clear whether "enemies" and "terrorists" are synonymous.

"Threat and Vulnerability"

This chapter of the *National Strategy* appropriately recognizes that the nature of our society—our "American way of life—makes us inherently vulnerable to terrorist attacks. It also acknowledges the imperatives not only of safeguarding our security and economy but also our culture, our civil liberties, democracy itself.

It appropriately, in our view, disaggregates chemical, biological, radiological, nuclear, conventional, and cyber attacks. But it suggests that chemical and biological weapons, generically, are "easy to manufacture," using "basic equipment." We have noted, in our threat assessments, including the one in this report, that such broad categorizations are unfortunate. Many of the more sophisticated chemical and biological weapons, especially those that could cause fatalities in the thousands or tens or thousands are very difficult to produce, maintain, and deliver.

It appropriately recognizes the potential damage that could result from an attack on U.S. agriculture.

"Organizing for a Secure Homeland"

This chapter of the *National Strategy* recognizes and explains the interconnected and interdependent roles of the Federal government, States and localities, the private sector, and the American people in a united national effort. It stresses the "vital need for cooperation between

[130] Ibid, p. 3.
[131] Chemical, biological, radiological, nuclear, and conventional explosives.

the Federal government and State and local governments . . . horizontally (within each level of government) and vertically (among various levels of government)."

In a move that we strongly endorse, it announces the intention to retain the White House Office of Homeland Security, even after the formation of the new Department of Homeland Security, with authority "to certify that the budgets of . . . executive branch departments will enable them to carry out their homeland security responsibilities."

It appropriately notes that the Department of Defense has important roles in homeland security, both for "homeland defense"—"military missions such as combat air patrols or maritime defense" in which the Department would "take the lead in defending the people and territory of our country—as well as "military support to civil authorities"—where the Department supports other agencies in responding to attacks, natural disasters, or "other catastrophies."

It appropriately, we believe, calls on the Governors of the several States "to establish a single Homeland Security Task Force (HSTF) for the state, to serve as his or her primary coordinating body with the federal government," but unfortunately does not offer to do the same in return. (We address this issue directly later in this report.)

"Intelligence and Warning"

This chapter correctly notes that appropriate assessments—both "tactical" and strategic"—of terrorist threats must precede any realistic assessment of our vulnerability. We are arguably infinitely vulnerable. Only when we can realistically determine what threats exist that would seek to exploit particular vulnerabilities will we be in position to take preventive and defensive steps and other appropriate responses.

Unfortunately, the *Strategy* does not suggest what products of the tactical or strategic (especially strategic) assessments will be produced or how and to whom such products will be disseminated.

We address, in considerable detail, the issues of intelligence collection, analysis, and dissemination and make specific policy recommendations with respect thereto, later in this chapter.

"Border and Transportation Security"

That chapter clearly and appropriately sets forth important initiatives for improving security at our borders and in our transportation systems. It notes the potential for using biometrics for improved identification, the criticality of deploying a border "entry-exit" system for foreign visitors, for increasing security with respect to commercial cargo entering the United States, for implementing "unified, national standards" for transportation security, for providing additional resources for the U.S. Coast Guard, and for improving visa processes.

On the latter issue, it suggests that the new Department of Homeland Security will "control the issuance of visas to foreigners" but provides no detail on how that will be accomplished.

"Domestic Counterterrorism"

Near the beginning of that chapter of the *National Strategy* is an explicit statement:

> *The U.S. government has not yet developed a satisfactory system to analyze information in order to predict and assess the threat of a terrorist attack within the United States.*

We fully concur and offer a specific recommendation later in this chapter directed at helping to solve that problem.

While discussing several tactical and operational approaches to address the challenges in this arena, this chapter does not, in our view, address some of the more strategic issues, such as the important relationship between the Department of Justice and the Department of Homeland Security and the critical role that State and local law enforcement have in this area. It also does nothing to address the proliferation of interagency and intergovernmental mechanisms, which seem not to be part of any overall design. We address that issue below, as well.

"Protecting Critical Infrastructures and Key Assets"

We applaud the policy decision, articulated in this chapter, to "unify the responsibility for coordinating cyber and physical infrastructure protection efforts" into the new DHS, especially for providing a single point of contact on such issues for States, localities, and the private sector.

The chapter also notes the intention to create a national infrastructure protection plan—a laudable goal—as well as the recognition of the international interdependencies of many critical infrastructures, especially in the transportation and cyber realms.

We also note with approval the careful articulation of Lead Agency responsibilities for critical infrastructure protection. We believe that that model should be applied to other functional areas for combating terrorisms and cite specific instances of that in other parts of this report.

We discuss those and related issues in considerable detail in Chapter VIII, below.

"Defending Against Catastrophic Threats"

We concur in the initiatives in this chapter for specific improvements in sensors and other detection and health surveillance capabilities. Those initiatives are fully consistent with specific recommendations contained in earlier reports of this panel.

The chapter acknowledges the need for improvements in laboratory capabilities but does not articulate specific proposals to address that issue. We do so, along with other policy recommendations, in our health and medical chapter later in this report.

"Emergency Preparedness and Response"

We concur strongly in the views expressed in the chapter on the different, separate response plans. We agree (as we have consistently expressed) that such plans should be merged. That chapter calls that proposed plan the "Federal Incident Management Plan." We suggest that the

better title would be *National* Incident *Response* Plan, which by its name would recognize the important role of States, localities, and the private sector. The accompanying proposal to establish a national incident management system certainly recognizes that, and the name of the plan should as well.

We wholeheartedly endorse the intention to develop a "national emergency communications plan" designed to establish "protocols, processes, and national standards for technology acquisition." We have previously recommended such a process for all emergency response equipment and systems. It is especially critical in the area of communications.

We also applaud the emphasis in that chapter of the *National Strategy* of improving both coordination with and the capabilities of the public health sector. We have previously made recommendations in this area, and make additional ones below, in our chapter on health and medical issues.

On the issue of military support to civil authorities, the parameters of which are outlined in this chapter of the *Strategy*, we devote a considerable amount of our Chapter IX, below, with several specific policy recommendations.

IMPROVING THE STRATEGY AND STRUCTURE

Intelligence Collection, Analysis, and Dissemination

Dealing with the Terrorists Among Us

It is now clear from contemporaneous reports and recent arrests that potential terrorists, perhaps in large numbers, are inside the United States. Many of them may have received training in foreign camps. They may seek to carry out more attacks against U.S. citizens and property. This new aspect of the terrorist threat requires a new approach in two key areas:

- The need for a focused and comprehensive analysis of threats of potential attacks inside the United States; and
- The need to address the gaps in collecting intelligence on foreign terrorists threats inside this country

The U.S. government's organization reflects an artificial distinction between "foreign" and "domestic" terrorist threats. The new threat environment, where those distinctions are increasingly blurred, requires a more robust and focused approach to all aspects of intelligence – collection, analysis and dissemination – whether it is collected at home or abroad. And this must be done in a way that respects American civil liberties.

The CIA, FBI, other members of the Intelligence Community, and the proposed Department of Homeland Security (DHS) will all have roles for intelligence-related functions. DHS will have responsibility only for vulnerability assessments for critical infrastructure protection, as well as for providing nationwide alerts. As things now stand, the FBI and CIA will each continue to have its own domain for terrorism intelligence with only marginal direct coordination between those entities, and no direct, formal relationship with the proposed DHS. Yet, such large, multi-mission agencies as the FBI and the CIA are incapable of changing direction quickly enough,

and should not be tasked further, to respond to current dangers. There is a risk of duplication, overlap, and bureaucratic "stovepiping" in this vital area. So a consolidation of certain activities is required.

Recommendation: That the President direct the establishment of a National Counter Terrorism Center (NCTC)

That entity should be a "stand-alone" organization outside of the FBI, CIA, or the DHS. The objective is to consolidate in one entity the analysis of foreign-collected and domestically-collected intelligence and information on international terrorists and terrorist organizations threatening attacks against the United States. This would be accomplished by permanently transferring (not "detailing") analysts currently performing those functions within the CIA (i.e., the core analytic capability within the CIA's Counter Terrorism Center), the FBI (the newly-expanded analytical section), other appropriate members of the Intelligence Community, representation from DHS (when formed), and supplementing with new hires as necessary.

The NCTC should be an Independent Agency of the Federal Executive Branch, similar to the standing of the Environmental Protection Agency, the Federal Emergency Management Agency, NASA, or the General Services Administration. The new entity should be a full member of the U.S. Intelligence Community. The agency head should be appointed by the President with the advice and consent of the U.S. Senate.

Advantages and Disadvantages of an Independent Agency

The members of the Advisory Panel discussed at length whether the NCTC should be placed within an existing department or agency or within the proposed Department of Homeland Security.

The panel discounted its placement in the Central Intelligence Agency for legal, policy, perception, and cultural reasons. The panel discussed and rejected the notion that this entity could be part of the FBI or an agency within the Department of Justice. Panel members felt that such placement would cause the entity to have too much law enforcement focus—building cases for prosecution—rather than detection and prevention.

The panel considered the prospect of placing the entity in the proposed Department of Homeland Security (DHS). While many panel members agree that such placement is a viable option, that alternative was eventually rejected for several reasons. First and most important, DHS will not be the only "customer" of the products of the NCTC. Other key Federal entities—notably the Department of Justice and its agencies, the Department of Health and Human Services, the Department of Defense, the Department of State, and the Department of Agriculture—will all require significant intelligence products from the NCTC. States, localities, and elements of the private sector will all be considerable consumers of NCTC products. Moreover, it would be viewed by other Federal agencies as being more responsive to DHS activities and priorities at the expense of other agencies' requirements. As a DHS entity, the NCTC would have to compete for resources with other DHS functions.

The panel concluded that a stand-alone entity, with its own funding, would be more likely to set priorities for its activities more objectively—an "honest broker" for competing requirements—and would not be viewed as tied to any single agency's mission.

The disadvantage to a stand-alone agency is that it may simply create more bureaucracy. That argument will be neither more nor less valid than the suggestion that DHS will create new bureaucracy. Moving existing resources and responsibilities from the FBI and from other entities in the Intelligence Community will minimize any real growth of government. The advantages gained in this structure outweigh any adverse impact, in the panel's view.

The NCTC would be responsible for the fusion of intelligence—from all sources, foreign and domestic—on potential terrorist attacks inside the United States. It would be responsible for the production and dissemination of analytical products to all appropriate "customers," including the Departments of Justice, Homeland Security, State, Health and Human Services, Agriculture, and Defense, and in coordination with those agencies, to designated and cleared officials in States, localities, and the private sector. It would have the authority to levy direct intelligence requirements on the Intelligence Community for the collection of intelligence on potential threats inside the United States. (See further discussion on collection below.)

The NCTC should be the entity that manages the "Collaborative Classified Enterprise" outlined in the *National Strategy for Homeland Security*, which links Federal, State, and local efforts in analyzing the activities of persons who have links to foreign states or to foreign terrorist organizations. The intelligence and information sharing functions currently being developed through the U.S. Attorney Antiterrorism Task Forces and slated to be moved to the proposed DHS should instead be imbedded in the NCTC.

The Critical Role of States, Localities, and the Private Sector

State and local entities, as well as key segments of the private sector, currently develop important intelligence and related information on potential terrorist threats to the homeland. No comprehensive system currently exists for consolidating all of that information into coherent threat analyses. To accomplish these functions and to establish other important coordination with States, localities, and the private sector, the NCTC staff should include significant representation from each of those segments. The panel envisions the NCTC hiring personnel with related experience at the State and local level and in the private sector, either on a permanent or rotational basis or a combination of the two. In addition, functions for developing guidance and for improving procedures should be informed by an advisory council consisting of senior officials from States (governors, State emergency managers, State police, State public health) localities (mayors, city managers, law enforcement, emergency managers, fire services, emergency medical technicians, and other local responders), and appropriate private sector entities (especially representatives from critical infrastructures). Moreover, formal operational relationships should be established with States and localities that have created structures and processes with similar missions that can be used as models for other areas of the country. Examples include the California Terrorism Information Center (CATIC), the Los Angeles Operational Area Terrorism Early Warning Group, and similar efforts in New York City.[132]

It is clear that the Federal government is far from perfecting a system of sharing national security intelligence and other information, developed at the Federal level, with States, localities, and certain segments of the private sector. While important progress has been made, the flow of intelligence and information is still not completely a "two-way street." The prevailing view continues to be that the "Feds" like to receive information but are too reluctant to share completely. Not all officials at every level of government need to be cleared for classified information. The Federal government must do a better job of designating "trusted agents" at the State and local level and in the private sector and move forward with clearing those trusted agents—at Federal expense. This should not be a case of the Federal government allowing those

[132] For additional information on the partnership of CATIC with the New York Police Department's Counter Terrorism Division and the Defense Intelligence Agency to share information and intelligence about suspected terrorist activities, see http://caag.state.ca.us/newsalerts/2002/02-107.htm, and "State Joins U.S., N.Y. to Fight Terror," by William Overend, Los Angeles (CA) Times, October 1, 2002.

agents access and then giving them the "privilege" of paying for it. This is a national requirement—not Federal on the one hand, and States, localities and the private sector on the other. Additional Federal resources are required, and soon, to make this process work.

Improving the Collection Function

Recommendation: That the collection of intelligence and other information on international terrorist activities inside the United States, including the authorities, responsibilities and safeguards under the Foreign Intelligence Surveillance Act (FISA), which are currently in the FBI, be transferred to the NCTC

This collection function would be functionally separate from, but physically co-located with, the analytical fusion component.

The panel makes this recommendation for two reasons. First, while the FBI remains the world's preeminent law enforcement agency, there is a big difference between dealing with a terrorist act as a crime to be punished and dealing with it as an attack to be prevented. We commend the FBI leadership for its efforts to make these changes. But the Bureau's long standing tradition and organizational culture persuade us that, even with the best of intentions, the FBI cannot soon be made over into an organization dedicated to detecting and preventing attacks rather than one dedicated to punishing them.

Second, even if the FBI could be remade, the panel believes it important to separate the intelligence collection function from the law enforcement function to avoid the impression that the U.S. is establishing a kind of "secret police."

The collection component of the NCTC should be based on the concept of the Foreign Terrorist Tracking Task Force created by the Attorney General in fall of 2002—multiple agency representation and robust technological capabilities—but with authority to collect intelligence and information within the United States. It would be authorized to collect intelligence only on international terrorism threats. It could not lawfully collect any other intelligence. Counter terrorism intelligence collection outside the United States would continue to be accomplished by the CIA, NSA, and other foreign IC components.

The NCTC would have no "sanction" authority. It would not have arrest powers—that authority will continue to rest with the FBI, other Federal law enforcement agencies, and State and local law enforcement. The NCTC would have no authority to engage in deportations or other actions with respect to immigration issues, to seize the assets of foreign terrorists or their supporters, or to conduct any other punitive activities against persons suspected of being terrorists or supporters of terrorism. The NCTC will provide information that can be "actionable" to those agencies that do have the authority to take action. A challenge will arise on those occasions when the NCTC will need to pass intelligence "cueing" to law enforcement agencies for the purpose of constituting an arrest. But the challenge will be fundamentally no greater than it is today when existing U.S. intelligence agencies "cue" Federal law enforcements agencies for such purposes.

This new collection component of the NCTC would operate under significant judicial, policy, and administrative restraints. It will be subject to the requirements of the Foreign Intelligence

Surveillance Act (FISA)[133] and the Attorney General's Guidelines for terrorism investigations. This component would be required to seek legal authority from the Foreign Intelligence Surveillance Court (FISC) for intrusive (surveillance or search) activities. Moreover, the NCTC would not require any expansion of the authority under FISA or the conditions and strictures that apply thereto, or additional authority beyond that contained in the USA PATRIOT Act. The FBI would continue to have responsibility for purely domestic terrorist organizations and for non-terrorism related organized crime. Title III wiretap responsibilities would remain with the FBI for criminal activities.

To ensure that the NCTC remained within these guidelines, a Policy and Program Steering Committee for the new agency should be established, consisting of the new agency's director, the Director of Central Intelligence, the Attorney General, and the new Secretary of DHS (when appointed and confirmed). The functions of the Office of Intelligence and Policy Review currently in the Department of Justice (DOJ) would move to the new NCTC to staff this steering committee, to assist in ensuring that the entity adheres to all relevant constitutional, statutory, regulatory, and policy requirements, and to assist in coordinating the activities of the new entity with the FBI, and other law enforcement agencies.

In addition, there could be more focused and effective Congressional oversight of the domestic collection and analysis functions. Currently, the oversight of the FBI's FISA and other domestic intelligence activities is split between the Judiciary and Intelligence committees in each House of Congress. Creation of the NCTC would clearly place the primary responsibility for oversight of that agency under the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Such a structure and improved oversight would likely provide an even better mechanism for protecting civil liberties than do current structure and processes. For that reason, the panel makes the following, related

Recommendation: That the Congress ensure that oversight of the NCTC be concentrated in the intelligence committee in each House

How will the NCTC enhance civil liberties protections?

- It will have no "sanction" authorities—law enforcement, prosecution, deportation, asset seizures, etc.
- It will improve Congressional oversight
- It will create more effective oversight mechanisms within the Executive Branch
- It will have internal and external safeguards that will be focused on intelligence issues

The panel recognizes that the creation of this new entity, the NCTC, cannot happen overnight. Nonetheless, its creation should begin immediately. Some may argue that we should not attempt to make this change in the midst of the "war on terrorism." But that war may continue for many years, and the danger now posed by terrorists underscores the need for moving ahead on an urgent basis. In the near term, the FBI will continue to have FISA and other domestic collection responsibilities. Deliberate and thoughtful planning will be required to ensure continuity and to

[133] 50 U.S. Code, Chapter 36 (50 USC Sections 1801-1863) (PL 105-511, October 25, 1978)

transfer effectively and as seamlessly as possible the capabilities and functions required for the NCTC. But, to underline the point, the NCTC should be established right away.[134]

The panel also recognizes that other agencies may continue to require some limited analytical capability. The NCTC will be responsible for strategic level intelligence analysis and for creating intelligence products that will inform operational decisions. Individual agencies, such as the FBI and the new DHS when formed, may need some internal analytical capability to take NCTC product and convert it from the operational level into tactical, actionable intelligence. It will be necessary, however, to ensure that other agencies do not seek to duplicate the NCTC

[134] Panel Chairman Jim Gilmore filed the following statement, in which he was joined by Panel Member Ellen Gordon, concurring in the recommendation with reservations:
"The Commission has devoted much time to the discussion of a new agency to collect information on international terrorist activities inside the U.S. My approach has been to maintain these functions within the FBI, and to build upon their considerable structures, sources and resources to upgrade and improve this function. After great discussion and testimony, the Commission has decided to recommend the creation of a new agency. I will support this recommendation, but only with the oversight provisions and legal requirements contained and described in the report, to ensure no diminution of the civil liberties of the People of the United States."
Panel Member Jim Greenleaf filed the following dissent:
"I am in favor of the creation of the NCTC but only for the analytical 'fusion' function. I am opposed to the creation of an independent organization within the NCTC that would collect intelligence and other information on international terrorists activities inside the United States.
"I believe that the FBI is fully capable of collecting the needed information in an effective, efficient, and lawful manner. The Bureau is like most bureaucracies and change comes slowly. However, knowing the caliber and dedication of the men and woman in the organization, they can meet these new challenges and make the appropriate adjustments to counter the terrorist threat.
"It will take years for a new organization to be created and become an effective resource in the fight against terrorism. The FBI already has agents in the field with the proper contacts to collect much of the needed intelligence. More certainly needs to be done. I am concerned about creating an organization that places detection and prevention ahead of prosecution. The FBI culture as a law enforcement agency provides a backdrop and check and balance against any abuse of civil liberties.
"Terrorism is a crime and needs to be addressed in that fashion following the current AG Guidelines and the Constitution. An organization designed to detect and prevent will not by definition be as sensitive and cautious in carrying out their mandate to protect civil liberties. I fully understand the restrictions that will be placed on the new agency, but doubt they can do the job required of them by operating in a very murky area of law and governmental guidelines. The issue of "secret police" becomes more of a factor for the new organization rather then with the FBI.
"Although the new organization would only collect intelligence on international terrorism threats, I find it difficult to visualize how they would carry out that mandate without involving domestic persons and organizations, since many cases involve both domestic subjects as well as international subjects. Many of the cases would evolve into complex relationships between domestic and international people and organizations, thus creating a difficult problem of jurisdiction and further concerns about 'stovepiping' between agencies.
"I am concerned about any agency that doesn't have to be held accountable for their actions by not having to defend their investigation by use of 'sanctions.' The ultimate arrest and prosecution of a subject acts as a logical process for the organization to demonstrate that they have operated within the law in conducting their business. Decisions made as to what course of action should be followed in order to 'detect and prevent' may very well result in a situation where the subject or subjects could not be prosecuted, thereby leaving the system with the question of what to do with them once the case becomes public knowledge. Certainly the prevention of a terrorist attack is of the highest priority, but what do we sacrifice in the process?
"I would prefer to see the FBI given additional resources especially in the area of computer support. They should place an increased emphasis on building a robust analytical capability to do a better job of recognizing and connecting the 'elusive dots' so they can provide valuable input to the NCTC. The AG Guidelines should also be revisited with the view of making them more 'user-friendly' and identify areas where lines can be drawn clearly and distinctly for aggressive investigative activity. Agents shouldn't have to worry about interpreting the rules. They need to know what is expected of them so they can go forward with an aggressive intelligence collecting process that is carried out in a way the American people would expect, and in a manner that the Constitution demands."

intelligence analytical fusion function, as has been the case in certain other historical contexts within the Intelligence Community. The President must ensure that the NCTC is the primary fusion center for all domestic intelligence. It must not be allowed to become a "coordinator of coordinators."

The panel is aware of other recent proposals that appear to be designed to address the collection problem. One was made by "The Task Force on National Security in the Information Age" of the Markle Foundation.[135] That proposal would place certain information collection functions in the proposed DHS, but would leave domestic intelligence collection with the FBI. We believe that that proposal does not go far enough in resolving the problem.

We are also aware of proposals similar to ours that are being made by U.S. Senators John Edwards (NC) and Bob Graham (FL).[136] The major distinction is that those proposals, while creating a separate collection entity, would leave that entity in the Department of Justice. For reasons stated above, we believe that the new entity must stand alone and clearly separated from law enforcement. Apparently, the Executive Branch is also considering some alternative to address the problem, reportedly including the establishment of something like an American version of the British MI5.[137] The panel has, however, avoided any comparison between our proposal and MI5. Our Constitution, our laws, our history, and our culture require a United States solution.

Collection Function—Summary of Key Points

- Would not *create* a domestic intelligence function; that function is already being performed by the FBI
- Would transfer that function to an entity with a detection and prevention, not law enforcement, focus and culture
- Would execute FISA and other foreign terrorist legal authorities inside the United States
- Would only effect persons with connections to foreign terrorists or terrorist entities, not purely domestic organizations or persons
- Would have no responsibility for non-terrorism related criminal activity
- Would *not* have arrest powers or other "sanction" authority
- Would be subject to requirements and restrictions in FISA (including application to the Foreign Intelligence Surveillance Court) and in the AG Guidelines
- Would not require new or expanded authority
- Would *not* have Title III wiretap authority
- Would be monitored by a steering committee and staff verification function (OIPR)
- Would likely provide better civil liberties and liberties protection
- Would have direct and significant relationships with States, localities, and the private sector

[135] *Protecting America's Freedom in the Information Age,* New York: Markle Foundation, October 2002.
[136] "Spies in the Ointment? Experts Debate Whether U.S. Should Launch Domestic Espionage Agency," CQ Homeland Security bulletin, *Congressional Quarterly,* Oct. 14, 2002.
[137] "U.S. may set up MI5-style spy agency in security shake-up." *The Telegraph* (U.K), October 31, 2002.

The Importance of Threat and Vulnerability Assessments

The *National Strategy for Homeland Security* appropriately notes the requirement for both strategic and tactical analysis and vulnerability assessments and designates various lead or co-lead agencies for those functions. The proposed DHS is only responsible for disseminating "real time actionable" information to others. It apparently has sole responsibility only for vulnerability assessments for critical infrastructure protection. There is no indication that strategic assessments of threats inside the U.S. will receive dissemination to State and local agencies.

Recommendation: That the President direct that the NCTC produce continuing, comprehensive "strategic" assessments of threats inside the United States, to be provided to policymakers at all levels, to help ensure appropriate planning and allocation of preparedness and response resources

The Role of the Department of Homeland Security in Intelligence Functions

It appears that the new DHS will have no authority for intelligence collection, limited capability for intelligence analysis, and significant responsibility for threat warnings.

Recommendations: That the Congress and the President ensure that the DHS has the authority to levy direct intelligence requirements on the Intelligence Community for the collection or additional analysis of intelligence of potential threats inside the United States to aid in the execution of its specific responsibilities in the area of critical infrastructure protection vulnerability assessments

That the Congress and the President ensure that the DHS has robust capability for combining threat information generated by the Intelligence Community and the NCTC with vulnerability information the Department generates in cooperation with the private sector to provide comprehensive and continuing assessments on potential risks to U.S. critical infrastructure

These capabilities will be important not only for the DHS specified missions but also for the DHS role in the NCTC.

Managing Operations

The *National Strategy for Homeland Security* has eliminated the distinction between "crisis" and "consequence" management. This will help remove certain ambiguities in the responsibilities and authority for planning and response. The creation of an overarching National Incident Response Plan to replace the Federal Response Plan and numerous other Federal plans can also clarify responsibilities. With the merger of the U.S. Customs Service (USCS), the U.S.Coast Guard (USCG), and the Immigration and Naturalization Service (INS)(and others) into the new DHS, that agency will have control over some but not all Federal law enforcement capability. The *National Strategy* provides that the Secretary of DHS will have the responsibility for "coordination and integration" of Federal, State, local, and private" activities for critical infrastructure protection (CIP). But it does not provide any vision about the extent to which DHS will be "in charge" of executing a response during or after an attack on some CIP sector;

nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one.

Recommendations: That the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies.

That situation is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, after DHS is formed, will be in charge in the event of a biological attack.

Recommendation: That the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism attack, and specify its responsibilities and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations

Interagency Coordination

There are numerous Federal interagency coordination structures and several combined Federal/State/local structures. As examples of the later, the Joint Terrorism Tasks Forces (JTTF) (FBI) will remain with the FBI and a new National JTTF (FBI) will be formed. But JTTFs are organized differently in various jurisdictions. And according to the *National Strategy*, the responsibilities (for intelligence/information sharing with State and local law enforcement) of the U.S. Attorney Antiterrorism Task Forces (ATTFs) will shift to the DHS. The proliferation of such mechanisms will likely cause unnecessary duplication of effort. More important, the *National Strategy* calls on the Governors of the several States "to establish a single Homeland Security Task Force. . .to serve as [the] primary coordinating body with the Federal government." But there is no similar call for a single mechanism at the Federal end.

Recommendation: That the Assistant to the President for Homeland Security review and recommend to the President, and that the President direct, a restructuring of interagency mechanisms to ensure better coordination within the Federal government, and with States, localities, and the private sector, to avoid confusion and to reduce unnecessary expenditure of limited resources at all levels

Legal Authorities

With the formation of the new DHS and other initiatives envisioned in the *National Strategy*, various statutory, regulatory, and other authorities (e.g., PDDs 37, 62, and 63) will be directly implicated. The *Strategy* appropriately calls for a review of legal authority for use of the military domestically. But other legal and regulatory issues must be addressed, not the least of which are quarantine, isolation, mandatory vaccinations, and other prescriptive measures that may be called for in the event of a biological attack.

Recommendation: That the President direct the Attorney General to conduct a thorough review of applicable laws and regulations and recommend legislative changes before the opening of the next Congress.

The Congress

The Congress is still not well organized to address issues involving homeland security in a cohesive way. The House recently took the bold, necessary, but unfortunately only temporary step of creating a special committee just to consider the proposal to create the Department of Homeland Security. Structures of that nature are required on a longer-term basis. Jurisdiction for various aspects of this issue continues to be scattered over dozens of committees and subcommittees. We therefore restate our prior recommendation with a modification.

Recommendation: That each House of the Congress establish a separate authorizing committee and related appropriation subcommittee with jurisdiction over Federal programs and authority for Combating Terrorism/Homeland Security

CHAPTER VI. IMPROVING HEALTH AND MEDICAL CAPABILITIES

Progress continues to be made with respect to health and medical care in response to terrorism in the United States. The infusion of nearly $1 billion dollars from the Department of Health and Human Services (DHHS) over the past year has done much to focus States and localities on developing a plan and building capabilities to respond to bioterrorism. There was a broad consensus among interviewed State and local public health and medical officials[138] that DHHS should receive high marks for distributing both the public health and hospital preparedness cooperative agreement funds efficiently and equitably. A number of interviewees commented that they had never seen the Federal government respond to any problem with such rapidity. This distribution of funds should serve as a shining example of how the Federal government can assist State and local governments and entities in terrorism preparedness. However, because the Constitution vests the power to act to preserve the public's health in the States as an application of their police powers,[139] the nation's health and medical preparedness cannot rely heavily on the Federal government. In addition, a review of DHHS[140] has shown that its anti-terrorism focus is primarily but not exclusively bioterrorism. While DHHS will clearly lead the technical and operational efforts to prevent, detect, and respond to bioterrorism, other types of terrorist attacks, such as those using chemical, radiological, conventional explosive, or nuclear devices, have significant public health and medical dimensions, and the preparedness for these should not be de-linked from that of bioterrorism.

The initial focus on bioterrorism was appropriate because biological terrorism had been virtually ignored prior to 1995. However, as the system has been strengthened to deal with bioterrorism DHHS goals should be broadened, and DHHS should have a comprehensive approach to terrorism response and prepare across the entire range of potential terrorism events. While interviewees stated that the bioterrorism preparedness grants will likely be applied to the full array of public health threats and, moreover, that other agencies and funding sources—including FEMA, local "first responders," and others—have addressed chemical, radiological, and explosive threats to a greater extent than bioterrorist ones, the Advisory Panel reiterates that response to all of these events should be integrated.

Supporting the view of the panel, an influential emergency preparedness policymaker argued that the bioterrorism preparedness program was misguided in that it further encouraged a "stovepiping" mentality among officials at all levels of government, which, in turn, inhibited them from "ratcheting up the dialogue to talk about the entire threat matrix." This individual went on to state that DHHS has done a poor job in integrating both its programmatic efforts and

[138] RAND interviewed seven federal health officials, five State and three local public health and emergency preparedness officials, five staff members of organizations representing State and local public health officials, two academics/health policy researchers, and one physician who directs several hospital emergency rooms in a major metropolitan area between June and October 2002 using a semi-structured interview protocol. The State and local health officials were drawn from agencies located in five States, and the emergency room physician worked in a sixth State.

[139] Gostin, L.O., J.W. Sapsin, S.P. Teret, S. Burris, J.S. Mair, J.G. Hodge, Jr., and J.S. Vernick, "The Model State Emergency Health Powers Act: Planning for and Response to Bioterrorism and Naturally Occurring Infectious Diseases," *JAMA*, 288(5), pp. 622-628.

[140] Reviews performed by RAND researchers and in Appendix J.

the public health perspective, in general, into the overall emergency response structure. Evidence to support this assertion was provided by a number of interviewees who maintained that DHHS has done a very poor job in coordinating activities with FEMA, in particular, as well as other Federal agencies, including the Departments of Justice, Agriculture, and State.

It is now essential that DHS, DHHS, OHS, and all other affected Federal agencies improve the planning, coordination, and implementation processes for all public health and medical efforts for combating terrorism.

Applying Resources Effectively

The President's FY03 budget request for bioterrorism is $5.9 billion with $4.3 billion allocated to DHHS. The President has allocated $1.2 billion to upgrade State and local capacity including: $591 million for hospital preparedness; $210 million for states to evaluate and improve their capacity to respond to bioterrorism; and $200 million to increase laboratory capacity at the State level. The President has also requested $300 million for management of the National Pharmaceutical Stockpile (NPS). These funds will also allow the United States to increase the supply of chemical antidotes and plan and train with the States for utilization of the stockpile. An additional $100 million is devoted solely to distribution and use of the smallpox vaccine. The President's budget recommends $392 million to improve our detection of and communication about bioterrorism-related outbreaks through improved communications. Of this amount, $175 million is designated for the acquisition of hardware and the provision of technical assistance to State and local public health providers.[141]

As noted above, funding has begun to flow to States and localities through DHHS bioterrorism preparedness grants, much of it directed toward public health. After years of cutbacks, State public health agencies' efforts to confront the terrorist threat are "beginning from a standing start."[142] Officials in public health have indicated that it will take at least a five-year commitment from DHHS, at approximately $1 billion per year to have a material impact on States and local government preparedness to respond to bioterrorist events. Interestingly, public health officials also believe that $1 billion is the "right" annual level, arguing that while the need to develop the public health infrastructure to better prepare for and respond to terrorist act was acute, it would be difficult to absorb the funds if the funding rate were increased appreciably. This stems in part from the difficulty of finding qualified people to fill newly-created positions, evaluating and purchasing new communications and information systems, and so on.

> As one state public health survey respondent noted: "Our State, like many others, is just establishing an infrastructure to administer the Federal resources available for bioterrorism preparedness and response."
>
> Another state public health survey respondent also commented, "We have a great plan to move forward and prepare the entire state health care system—we just need the staff to carry out."

[141] Office of Management and Budget, "Budget for FY03 ," The Office of the President, Washington, DC, http://www.whitehouse.gov/omb/budget/FY03/bud05.html, last accessed December 10, 2002.
[142] Inglesby, 2002

Multi-year funding, in addition to providing the required resources and allowing sufficient time for the States and locales to hire staff and to acquire new equipment, is critical in allowing States and local governments to attract and retain first-rate individuals and to invest an appropriate amount of money in new technologies. Many reported that long-term funding uncertainties presented a formidable barrier in their attempts increase their levels of preparedness. This problem is further exacerbated by the presence of severe State budget constraints, which increase the difficulties associated with making long-term plans.

> As one state public health survey respondent commented, "With the introduction of increased federal funding, we saw a REDUCTION of State funding."

Several respondents noted that DHHS even failed to prioritize the various components of the cooperative agreements, leaving State and local official in a quandary over where they should devote their resources. Additionally, DHHS has not effectively defined roles for Federal, State, and local public health officials. Moreover, with the exception of the hospital preparedness cooperative agreements that require States to work with hospitals, DHHS has offered States virtually no guidance on how, and with whom, to establish private sector partnerships.

> As one local public health department survey respondent noted, "From a Health Department's local perspective, the critical issues are 1) private cooperation and 2) "dual use" of new resources. At the Federal level, guidance regarding public/private health response tends to be inadequate, overly prescriptive, or otherwise unhelpful."

As an example of the difficulty facing States in recruiting qualified personnel, some State health department representatives reported major difficulties finding and hiring qualified epidemiologists, although little is known about the actual number of epidemiologists needed within the public health system, because no empirical studies have explored this to date. In one State, recruitment for epidemiologist positions has been "spotty"; the department often does not draw any "stellar" applicants. Individuals who apply for the positions are generally not trained epidemiologists, but have instead been veterinarians, statisticians, and individuals with doctorates in related areas. During a discussion of bioterrorism and public health at the American College of Epidemiology meeting in September 2002, panelists and other meeting participants used the fall 2001 experience to illustrate the interface between epidemiology and bioterrorism, and participants reiterated the great need for epidemiologists to fill positions in State and local health departments created by recent Federal funding programs.

Recommendation: That DHHS continue to provide financial support on the order of $1 billion per year over the next five years to strengthen the public health system in the United States

Attention should thereafter be paid to sustaining these resources beyond this time to maintain the system at a well-functioning level.

Recommendation: That DHS coordinate and centralize the access to information regarding funding from various agencies such as DHHS (including CDC), EPA, USDA, and others and simplify the application process

This centralization and simplification of grants processes is essential to eliminate confusion and unnecessary redundancies. (See our related, broader recommendation on this issue in Chapter IV, Resourcing the National Effort.)

Establishing and Using Metrics

In addition to providing significant resources for strengthening the public health sector, the Federal government should place renewed emphasis on multiyear funds to State, local, and private sector medical facilities to improve preparedness across the spectrum of response capabilities. All of these efforts must be evaluated with defined metrics to ensure the money is actually enhancing preparedness and that the resources are appropriate to the mission.

While many resources are being used to enhance capabilities to respond to terrorism, there is currently no framework in place for monitoring the States' progress in meeting the objectives of the cooperative agreements program and for evaluating States' performance with respect to various outcomes, although Federal officials have indicated that they are working to develop evaluation protocols. Moreover, there is a general lack of understanding on the part of representatives from State and local governments on precisely what they will be held accountable for and how their programs will be evaluated. Many of the respondents voiced a high level of frustration with the lack of evaluation plans from DHHS. One observer noted that DHHS needs to develop a common taxonomy for measuring program, as opposed to fiscal, accountability. Others expressed concern over the need for DHHS to articulate appropriate programs outcomes, how one would go about measuring progress towards reaching them, and a time line for achieving particular milestones.

Recommendation: That DHHS, in consultation with State, local, and private sector stakeholders, establish and implement a formal process for evaluating the effectiveness of investment in State, local, and private preparedness for responses to terrorist attacks, especially bioterrorism

In the absence of Federal criteria, some national organizations are developing competencies by which health departments can gauge their level of preparedness, beyond workforce preparedness. For example, the National Association of City and County Health Officials (NACCHO) is working with public health partners "to develop a module of performance measures, as part of the National Public Health Performance Standards Program, that will assist communities in assessing their capacity to respond to bioterrorist disease threats."[143] The goals of this project are to identify possible capacities, prioritize these capacities, and gather the input of stakeholders with the aim of reaching consensus. This is the first attempt at developing a potential credentialing process for public health departments, and the group hoped to implement field tests in late fall or early winter 2002.

Additionally, there are not yet widely agreed metrics by which to assess levels of preparedness among the workforce, although there are some aimed at particular sectors. There is not even a single definition of a "prepared workforce" because there is no consensus on what being prepared is. According to the U.S. General Accounting Office (GAO), as of 2002, "There is no

[143] National Association of City and County Health Officials. 2002. National Public Health Performance Standards Program. Available at http://www.naccho.org/project48.cfm accessed November 14, 2002.

consensus on the optimal number and ratio of health professionals needed to meet the population's health care needs,"[144] Those who RAND interviewed[145] for the study seemed inclined to use the "critical capacities" outlined in CDC's bioterrorism funding guidance to States as benchmarks for their success in preparing the workforce for bioterrorism specifically following receipt of funding.

While it is important to evaluate programs, it is particularly challenging given the low likelihood of a bioterrorism event. There have fortunately been few incidents to test workforce preparedness in real life situations. Nevertheless, some measure of requirements identification and an evaluation of the preparedness to meet those requirements must be accomplished before incidents occur.

Recommendation: That DHHS fund studies aimed at modeling the size and scope of the healthcare and public health workforce needed to respond to a range of public health emergencies and day-to-day public health issues

This type of modeling will help to develop a goal or baseline of preparedness so that during evaluations actual readiness can be compared to the preparedness goal. Without the kind of data that will result from such studies, it is impossible to quantify the gap between the current workforce and a workforce "prepared" to address these issues.

Improving Hospitals and Other Medical Facilities

DHHS bioterrorism preparedness grants have begun to address public health shortfalls; hospitals and other medical facilities are less prepared. A nationwide survey of hospital emergency departments conducted by RAND on behalf of the Gilmore Commission just prior to September 11, 2001, found that only 32 percent of hospitals indicated they had plans or standard operating procedures (SOPs) that address a moderate-sized biological incident, whereas 54 percent reported having a plan or SOP in place for a moderate-sized chemical incident.[146] Similarly, a 1998 survey of hospital emergency departments in four northwestern States found that found that fewer than 20 percent had plans in place for addressing chemical or biological events, less than half had integral decontamination units, and most did not have adequate respiratory protective equipment for the emergency departments' staff.[147] A second, follow-up survey conducted by RAND just prior to the anniversary of September 11 found that while 30 percent of hospitals have increased or shifted staff since the attacks to focus on bioterrorism and other Weapons of

[144] U.S. General Accounting Office. 2001. Health workforce: ensuring adequate supply and distribution remains challenging. Report No. GAO 01-1042T. Available at http://www.gao.gov/ accessed September 15, 2002.
[145] Fourteen individuals involved in enhancing workforce preparedness at various levels (State health department, trade association, Federal government) were interviewed to learn about their activities, concerns, and unmet needs around response to the potential threat of terrorism, bioterrorism, and other public health emergencies. We developed two formal interview scripts—one for State health officials and another association or academic institution representatives. Our interviews with Federal officials were organized around questions related to specific Federal initiatives. Each interview lasted approximately one hour. Four were conducted in person, and the rest via telephone.
[146] Davis, L.M. and J.C. Blanchard, *Are Local Health Responders Ready for Biological and Chemical Terrorism?* IP-221-OSD, RAND, 2002.
[147] Wetter, D.C., W.E. Daniell, and C.D. Treser, "Hospital Preparedness for Victims of Chemical or Biological Terrorism," *American Journal of Public Health*, Vol. 91, pp. 710-716, 2001.

Mass Destruction (WMD) preparedness issues, only 33 percent of relevant hospital personnel[148] have been trained to date on WMD awareness of response (see Appendix D—Survey Information and Analysis). This represents a significant increase from the 5 percent of relevant hospital personnel trained in WMD awareness and response prior to September 11, 2001.

Findings from the second RAND survey also supported the idea that public health and not the medical response has been the focus of Federal resources for bioterrorism preparedness to date. Only 20 percent of hospitals indicated that since September 11, 2001, they have received an increase in funding or other resources to address WMD preparedness in FY02, in contrast to the more than 70 percent of local public health departments that received an increase in funding or other types of resources. In FY03, just over 30 percent of hospitals expect to receive additional funding, while more than half of local public health departments expected an increase in the new fiscal year (See Appendix D).

> *"If additional funding is not provided to hospitals, the cost of WMD preparedness will be difficult if not impossible to meet."* A local hospital responder, second survey

> *"We are a rural medical facility. Financial survival is difficult in the current climate. Funding is not available for training…"* A local hospital responder, second survey

In contrast to the public health cooperative agreements, the hospital preparedness cooperative agreements were viewed as being inadequately funded (i.e., $125 million for FY 2002), with many, if not most, of the respondents arguing that DHHS, and HRSA in particular, has unrealistic expectations for their program, as articulated in the guidance documents, given what was viewed as a relatively meager level of support.

Because relatively little money—on average, approximately $25,000 per year—will be available for individual hospitals, several respondents noted that there may be a tendency to "go for the low-hanging fruit," in the words of one, and purchase communications or decontamination equipment in instances where the money could better be used, say, to increase surge capacity, to upgrade and expand information technology systems, and to improve coordination among local hospitals and health care providers. In fairness, Federal officials have recognized the inadequacy of the funding level. As a result, they have requested $500 million for FY03. Still, some experts believe that even this level of funding would not be sufficient to prepare the nation's 5,000 hospitals to handle mass casualty events, mainly because hospitals, like public health agencies, have responded to fiscal pressures by cutting back on staff and other resources and otherwise reducing "excess capacity."[149] The American Hospital Association estimated that it would take approximately $11 billion to ensure the preparedness of the nearly 5,000 hospitals throughout the nation.[150] In Colorado, initial DHHS funding amounted to $24,000 per hospital, FY03 funding

[148] Survey respondents were asked to indicate what percent of their hospital personnel who deal with acute response, environmental health, or coordination of emergency medical response had been trained in WMD awareness or response (particularly for incidents involving biological weapons).

[149] O'Toole, T. "Department of Health and Human Services Budget Priorities for FY03," testimony before the U.S. House of Representatives Budget Committee, February 28, 2002.

[150] In testimony to the Committee on Government Efficiency, Financial Management, and Intergovernmental Relations, Larry Wall, President of the Colorado Health and Hospital Association, member of the Governor's Expert Epidemic Emergency Response Committee, and Chairman of the Hospital Preparedness Advisory Committee, on August 18, 2002, the hospitals must address preparedness issues in at least eight areas: communication and

will provide an addition $46,000, but necessary improvements in communications alone would cost approximately $37,500 for a non-metropolitan hospital and $75,000 for a metropolitan hospital. [151]

Recommendation: That DHHS conduct a comprehensive assessment of the resources required by the nation's hospital system to respond to terrorism, and recommend appropriate Federal-State-Local-Private funding strategies

As part of that process, DHHS should, of course, consider recommendations of national organization like the American Hospital Association, but its assessment should be objective and independent.

Enhancing Communications

DHHS funds several programs aimed at improving the level of electronic connectivity among public health organizations. Examples of these programs include the Laboratory Response Network (LRN), which connects more than 80 public health laboratories in order to quickly identify pathogens used in bioterrorist attacks; the Health Alert Network (HAN), an Internet-based communications system to facilitate information sharing and distance-learning that links public health departments covering more than 90 percent of the nation's counties; the National Electronic Data Surveillance System (NEDSS), a Federal initiative aimed at promoting the adoption of data and information system standards in disease surveillance systems used at the Federal, State, and local levels; and the Epidemic Information Exchange (Epi-X), a secure, Internet-based system that enables State health departments to communicate with CDC. These information systems are focused on connecting public health entities but lack connectivity with medical, emergency services, and public safety officials. Interviewees pointed out that the CDC needs to assist in coordinating and connecting some of its own laboratory and disease surveillance information systems initiatives (e.g., NEDSS, LRN, HAN, Epi-X).

Recommendation: That DHHS continue to strengthen the Health Alert Network and other secure and rapid communications systems, as well as public health information systems that generate surveillance, epidemiologic and laboratory information

These information systems should be connected to provide circular information flow. A complete circle of communications is required, not a one-way or even two-way flow of information. This need was recognized in part in three of the 14 critical benchmarks in DHHS' bioterrorism preparedness grants:

---

notification; disease surveillance, disease reporting and laboratory identification; personal protective equipment; facility enhancements; dedicated decontamination facilities; medical/surgical and pharmaceutical supplies; training and drills; and mental health resources. Available at http://reform.house.gov/gefmir/hearings/2002hearings/0823_denver/wall_testimony.doc accessed December 2, 2002.

[151] Wall testimony.

"10.Develop a plan to improve working relationships and communication between Level A (clinical) laboratories and Level B/C laboratories, (i.e., Laboratory Response Network laboratories) as well as other public health officials.

11. Prepare a timeline for a plan that ensures that 90 percent of the population is covered by the Health Alert Network (HAN).

12. Prepare a timeline for the development of a communications system that provides a 24/7 flow of critical health information among hospital emergency departments, State and local health officials, and law enforcement officials."[152]

The development of an all-inclusive communications system would enhance the ability of officials to recognize, communicate, and respond to natural disease outbreaks as well as terrorist threats.

Improving Exercises

In our previous reports, we recognized that exercises are critical to ensure adequate training, to measure readiness, and to improve coordination among all responding entities. While various funding streams may encourage fragmentation of resources, exercises can be used to bring the pieces together as a functional whole. Common elements in exercises taking place in different parts of the system will be important for comparing performance among entities to ensure "system wide" capacity and serve as opportunities for testing how well the roles of these entities fit together in the overall coordinated response.

The second RAND survey, indeed, has found that since September 11, 2001, a majority of local health organizations (65 percent of local public health departments and 80 percent of hospitals) have participated in different types of field or tabletop exercises, particularly for chemical or biological incidents and for natural disasters. In addition, nearly all State public health departments since September 11, 2001, have participated in such exercises, particularly related to bioterrorism or chemical incidents (See Appendix D).

However, resources directed to State and local entities to conduct these exercises have been limited and incentives for cross discipline coordination require strengthening. We restate a previous recommendation with a follow on:

Recommendation: That the Congress increase Federal resources for appropriately designed exercises to be implemented by State, local, private sector medical and public health and emergency medical response entities

A variety of issues should be integrated into exercises. For example, the American Nurses Association (ANA) is concerned about personal protective issues as important considerations in their ability to respond to bioterrorism attacks. Nurses have voiced concerns about not being able to reach their children in the event of a hospital lockdown. The American Hospital Association has been involved in leading joint role-playing activities and developing guidelines around the workforce issues that need to be addressed to enhance the ability to respond to events.

[152] U.S. Department of Health and Human Services, HHS Fact Sheet, June 6, 2002

For example, they have recommended getting various community organizations involved in planning and thinking about who could check on healthcare providers' children in the event of an attack.

Perfecting Specialized Response Teams

The National Disaster Medical System and the Metropolitan Medical Response System attempt to provide surge and specialized health related assets to victims of natural and manmade disasters. On November 1, 2002, DHHS announced $2 million in grants to 42 communities to create local Medical Reserve Corps (MRCs), which are designed to help communities prepare for and respond to public health emergencies.[153] The MRC program is administered by the Office of the Surgeon General, although all MRCs will be developed, managed, and sustained at the local level. Additionally, the ANA is working with DHHS to develop National Nurses Response Teams (NNRT), which will consist of 200 nurses per region (2,000 nurses in total) who will receive standardized education aimed at preparing them to assist with mass vaccination and chemoprophlyaxis efforts. Finally, the American Pharmaceutical Association is working with DHHS's Office of Emergency Preparedness and several colleges of pharmacy to develop National Pharmacy Emergency Response Teams (NPRT). The goal of the program is to sign up and credential 2,000 pharmacists who can be mobilized to help respond to public health emergencies. However, it is not clear that enough professionals or equipment are available to staff and equip these teams, or how the teams will work together in the event of an emergency. An urgent need exists to clarify the role and functions of these various teams and the extent to which their roles will be coordinated at the Federal, State, and local levels.

Recommendation: That DHHS clearly articulate the roles, missions, capabilities and limitations of special response teams; that a plan be developed for the effective integration of such teams; and that focused training for special teams emphasize integration as well as coordination with States and localities

Promoting Technical Assistance

While public health and medical experts interviewed by RAND generally believed that they were provided a sufficient level of resources to begin establishing a reasonable capacity for responding to a bioterrorist attack, many felt that they lacked the expertise for, among other things selecting among competing technologies, developing templates for communicating risks and information on actual events to the public, developing plans for surge capacity and pharmaceutical distribution, and providing adequate training to staff.

All of this has been exacerbated by the aggressive vendors who have been inundating State and local officials with promotional materials and requests for meetings. Along these lines, a number of interviewees suggested that Federal officials should make a greater effort to establish standards for communications systems, information technologies, and even laboratory protocols.

Recommendation: That DHHS evaluate current processes for providing required technical assistance to States and localities, and implement changes to make the system more responsive

[153] HHS Release—"Medical Reserve Corps Units," November 1, 2002, HHS Press Office.

Increasing Surge Capacity

The medical system lacks the surge capacity that might be needed in the event of a terrorist attack. Because of the financial realities of medical insurance and managed care, hospitals operate on tight budgets. Facilities have eliminated beds and pharmaceuticals and face substantial workforce shortages.[154] DHHS has not asked States to develop workforce surge capacity, *per se*, but is requiring each State to be able to staff 500 critical beds per region in 2002 and 1,500 by 2003. DHHS has not provided models, algorithms, or other guidance as to how and where to locate the beds and how to staff them: State and local governments need to figure out how best to achieve this. The exception is the guidance that DHHS recently provided to States regarding setting up and staffing smallpox mass vaccination clinics. The Smallpox Vaccination Clinic Guide, released in September 2002, provides specific guidance regarding the number and type of clinical staff needed given specific assumptions about the number of individuals who would seek vaccination following a known smallpox attack.[155]

Some State public health officials are unclear about their role in assisting with planning for the staffing of hospital beds in the State and otherwise becoming involved in surge capacity issues, although they do work closely with some hospitals. One stressed that assessing and staffing needs, gaps, and issues in a large State are overwhelming at the State level and really needs to be addressed at the local/regional level. However, one State health department is playing a role by hiring an emergency room planner and pharmacist who will have primary responsibility for planning with hospitals around potential use of the National Pharmaceutical Stockpile (NPS).

Recommendation: That DHHS develop an electronic, continuously updated handbook on best practices in order to help States and localities more effectively manage surge capacity, the distribution of the NPS, and other preparedness goals [156]

In addition to hiring new staff, States are implementing a wide range of preparedness activities but have had little opportunity to share this information with colleagues in other States. Most involve training activities to enhance health department employees' basic public health and emergency preparedness skills. For example, the second RAND survey found that nearly three-quarters of hospitals and more than 80 percent of local public health departments indicated that since September 11, 2001, they had trained personnel on emergency response and preparedness for bioterrorism and/or for WMD, in general (See Appendix D). In addition, the case study interviews found that one department is providing training to epidemiology staff at the local level and is strongly emphasizing infrastructure development. For example, State lab capacity is being fostered through funding of laboratory enhancement activities at the regional level. Another State started an intensive, five-day field epidemiology course, to which members of their new regional response teams were invited. The course covered surveillance, statistics, infectious disease, and enhancing communication skills and had a key goal of getting the new hires to "think the same way." Several interviewees noted unique aspects of their States' plans from

[154] Tucker, Jonathan, "What the Anthrax Attacks Should Teach Us," *Hoover Digest*, 2002, No. 1, available at http://www-hoover.stanford.edu/publications/digest/021/tucker.html accessed on November 6, 2002.
[155] *Smallpox vaccination clinic guide: logistical considerations and guidance for State and local planning for emergency, large-scale, voluntary administration of smallpox vaccine in response to a smallpox outbreak*, DHHS, September 16, 2002.
[156] This could be modeled after the DHHS database on best practices in retaining the long-term care workforce available at http://www.directcareclearinghouse.org/practices/index.jsp

which other States might draw ideas if they were aware of them. One State, home to a very large metropolitan area and well as very impoverished areas, is acutely aware of the need to develop preparedness capacities across the entire State, which is a major challenge. A lot of pressure comes from large communities to make preparedness efforts population-based, but the interviewee noted that attention must also be paid to the rural areas of the State—which are also potential sites of manmade and natural public health emergencies. Another noted that the level of collaboration with the veterinary community in their State is fairly unique. DHHS should leverage these State and local initiatives to develop the best practices.

Federal, State, and local agencies, as well as many private sector entities, have not articulated, and therefore do not share, a common understanding of the meaning of a "prepared workforce." DHHS and other agencies should fund research and information sharing aimed at better understanding what a workforce "prepared" to address a range of health threats would look like in size, competencies, composition, and geographic distribution to allow implementation of best practices.

Providing One-Stop Shopping

Several respondents noted that there is still considerable uncertainty regarding the roles of the CDC and the Office of Public Health Emergency Preparedness (OPHEP) in coordinating DHHS bioterrorism preparedness activities. This uncertainty has led to a number of problems on the part of State and local public health officials, and this may be exacerbated as OPHEP moves from DHHS to DHS. Several officials expressed a high level of frustration with respect to the ability to gain access to, and communicate with, Federal officials who are in a position to render timely decisions on a range of issues. In other words, DHHS has not yet been able to offer cooperative agreement recipients "one-stop shopping." As a result, State and local public health officials reported that they often find themselves in the position of searching for appropriate contacts in the OPHEP, CDC, OEP, and HRSA to have their questions answered and to obtain technical assistance. Finally, a number of key policymakers pinpointed information technology as an area in desperate need of a long-range vision and plan, with one observer noting that despite years of trying, CDC has been unable to create a unified public health information system. This individual went on to describe the current patchwork of such systems simply as "a mess."

Enhancing Research

The National Institute of Allergy and Infectious Disease (NIAID) will be spending more than $1 billion dollars on new and improved prophylaxis and treatment for bioterror agents. While this is a considerable sum of money it should be recognized that it could take up to $800 million dollars and 10 to 15 years to develop one new vaccine. In addition to research on prevention, treatment, and cures, research is also required in applied public health to provide insight into the best way to get people to follow an antibiotic regimen, for example. In the aftermath of the anthrax attacks, only 44 percent of those instructed to complete a 60-day course of Cipro actually did

so.[157] This does not bode well for quarantine, isolation, vaccination, or other public health measures.

Recommendation: That NIH, in collaboration with CDC, strengthen programs focusing on both basic medical research and applied public health research, and the application of new technologies or devices in public health; and that DHS and OHS, in cooperation, prioritize and coordinate research among NIAID, other NIH entities, and other agencies conducting or sponsoring medical and health research, including DoD, DOE, and USDA, to avoid unnecessary duplication

Enacting Legal and Regulatory Changes

The Model Health Powers Emergency Act, a model law developed for the Federal Centers for Disease Control and Prevention and provided to State legislatures last year, would give authorities the right to enforce quarantines; vaccinate people; seize and destroy property without compensation; and ration medical supplies, food, and fuel in a public health emergency. It has been adopted by more than a third of States while being rejected by at least 22 States. This model law seeks to modernize outdated public health laws enacted before the development of modern medical technology and to incorporate civil liberties issues.

Many States that have adopted it are in a holding pattern, waiting for the Federal government to organize itself to deal with bioterrorism before operationalizing the legislation. The Federal Health Insurance Portability and Accountability Act (HIPAA) is in part designed to keep information about patients confidential and defines narrowly the information and the circumstances under which that information can be released. The public health community is exempt from these regulations, and therefore, during a public health emergency, medical information can be shared with public health agencies. However, during investigations into potential bioterror events, the goals and operating procedures of health and medical and public safety officials often conflicts. For instance, medical personnel are focused on identifying the cause of disease outbreaks and often are not familiar with preserving evidence using a chain of custody. Law enforcement officials gather evidence as the basis for criminal prosecution and may not consider the need for disease related testing. There are no mechanisms that encourage the integration of law enforcement and public health investigations, both of which may uncover evidence that ultimately can be presented in a court of law or may require disease testing. The relationship between the public health agencies and law enforcement in these situations—especially around the sharing of individually identifiable data—needs to be clarified. Although State and local involvement is critical, the Federal government needs to create and maintain some level of uniformity in dealing with these situations.

Recommendation: That each State that has not done so either adopt the Model Health Powers Emergency Act, as modified to conform to any single State's special requirements, or develop legislation of its own that accomplishes the same fundamental purposes; and work to operationalize laws and regulations that apply to CBRN incidents—naturally occurring, accidental or intentional, especially those that may require isolation, quarantine,

[157] Altman, Lawrence, K. "Many Workers Ignored Pill Regimen," *New York Times*, October 30, 2002, available at http://www.nytimes.com/2002/10/30/health/30ANTH.html accessed on November 6, 2002.

emergency vaccination of large segments of the population, or other significant emergency authorities

Recommendation: That the Congress clarify the conditions under which public health agencies, EMS, and hospitals can share information with law enforcement officials in special emergency circumstances under HIPAA

Such special circumstances would include instances, for example, where public health or medical providers have reason to believe that a person being treated for an illness may be involved in the intentional spread of a communicable disease or where it is necessary to provide law enforcement assistance in tracking relatives or other individuals who may have been exposed to an infected person.

Recommendation: As a prerequisite for receiving Federal law enforcement and health and medical funds from the Federal government, that States and localities be required to develop comprehensive plans for legally-appropriate cooperation between law enforcement and public health, EMS, and hospital officials

A carefully-crafted fusion center at the State level for the sharing of information between law enforcement, public health, medical officials, and other emergency responders, which has appropriate safeguards for ensuring confidential information to the maximum extent possible is is a potential model.

Determining Who Is In Charge

The OHS is working to create an overarching National Incident Response Plan to consolidate and replace the Federal Response Plan and numerous other Federal plans that may be invoked during a terrorism or disaster response. This plan will serve to ensure better clarity of purpose and better understanding of responsibilities. The *National Strategy* provides that the Secretary of DHS will have the responsibility for "coordination and integration of Federal, State, local, and private" activities for critical infrastructure protection (CIP). It does not, however, provide any vision about the extent to which DHS will be "in charge" of executing a response during or after an attack on some CIP sector; nor does it specify which Federal agency is in charge for the Federal sector for other types of attacks, especially a biological one. Earlier in this report, we made specific recommendations that bear repeating here.

Recommendation: That the President and the Congress clearly define the responsibilities of DHS and other Federal entities before, during, and after an attack has occurred, especially any authority for directing the activities of other Federal agencies

That situation is especially problematic when it comes to a bioterrorism attack. No one in the Federal structure can currently identify who is or, after DHS is formed, will be in charge in the event of a biological attack.

Recommendation: That the President specifically designate the DHS as the Lead Federal Agency for response to a bioterrorism attack, and specify its responsibilities

and authority before, during, and after an attack; and designate the DHHS as the Principal Supporting Agency to DHS to provide technical support and provide the interface with State and local public health entities and related private sector organizations

Establishing Public Communications Strategies

Last year the panel recognized the critical role of a well-designed public affairs strategy in informing the public, minimizing psychological impacts, and preventing the spread of misinformation in the event of a public health emergency. The communications response to the anthrax attacks of last fall demonstrated that Federal, State and local officials were not coordinating their statements, and this led to mistrust among the public, especially postal workers in Washington, DC. The development of a clear Federal strategy in coordination with State and local medical, public health, and elected officials is not evident.

Recommendation: That DHHS, in coordination with DHS, develop an on-going, well coordinated strategy for education of the public on the prevention, risks, signs, symptoms, treatments, and other important health and medical information before, during and after an attack or large-scale naturally occurring outbreak occurs

The strategy should include elements at the national, State, and local levels. This campaign should be led by a person or persons with medical and/or public health expertise with guidance from experts in risk communications as well as State and local emergency management and elected officials.

Additionally, much is still not known about the most effective ways to treat people with mental or emotional problems following a terrorist attack.

Recommendation: That DHHS, through the National Institute of Mental Health, and in collaboration with CDC, enhance funding for research into the prevention and treatment of the short and long-term psychological consequences of terrorist attacks[158]

This should include a special focus on biological terrorism and include agricultural terrorism as well as chemical and radiological terrorism and address strategies to be used before, during, and after an attack to minimize the negative psychological impacts. This research should also take into account the impact of public affairs and public communication strategies on various

---

[158] NIH issued a grant notice on July 24,2002 for the Rapid Assessment Post-Impact of Disasters grants under the Traumatic Stress Research Program available at <http://grants.nih.gov/grants/guide/pa-files/PAR-02-133.html> accessed December 2, 2002. The Bioterrorism Preparedness and Response Act signed by President Bush in June of 2002 includes $1.6 billion which does not cover research but includes some funding for mental health in the following areas: creation of a National Advisory Committee on Children and Terrorism within DHHS; enhanced strategies by the Department of Veterans Affairs for mental health counseling, including counseling to emergency response providers; addition of behavioral psychology experts to the Emergency Public Information and Communications Advisory Committee; educational grants for underserved professions to appropriate organizations for bioterrorism and emergency response; and creation of health professionals volunteer registry. M. Dittman available at http://www.apa.org/monitor/sep02/bioterrorism.html

segments of the population, including healthcare workers and other emergency responders. The panel notes that, in the past, research has emphasized such acute events as bombings, but little research has been conducted on the psychological consequences of ongoing events when people do not know when they are going to end.

Reconciling Interagency Issues

The Intelligence Community is not well equipped to assess threats that would have a direct impact on the public, especially as a result of bioterrorism. It is not well connected to health and medical experts and facilities involved in this field, in part because of a lack of security clearances held by those health and medical officials. In-house health and medical expertise in the Intelligence Community is not sufficiently robust to provide for continuing strategic assessments of bioterrorism cause and effect.

Recommendation: That the Intelligence Community improve its capacity for health and medical analysis by obtaining additional expertise in the medical and health implications of various terrorist threats

Enhancing Pharmaceutical Supplies and Distribution

The FY03 budget provides $65 million in grants to States for the implementation of distribution systems for pharmaceuticals through the National Pharmaceutical Stockpile (NPS). States are concerned about the their ability to receive and distribute products from NPS, which is composed of twelve 50-ton "Push Packages" of medical supplies placed throughout the country that can be deployed to any location within 12 hours. The NPS program is also responsible for storing and distributing smallpox vaccine. Once packages from the NPS arrive at an airfield, CDC transfers authority for managing the contents of the packages to State and local officials. Federal officials have indicated that a number of States came up short in their cooperative agreement proposals with respect to their plans for stockpile receipt and distribution. Federal technical assistance is needed on the part of State and local health officials to develop and exercise these plans. The panel acknowledges recent Federal efforts but suggests that additional enhancements as well as ways of measuring the ability of States to distribute the NPS are still in order.

Recommendation: That DHHS significantly enhance technical assistance to States to help develop plans and procedures for distributing the NPS, continue to require exercises that demonstrate the States' ability to employ the NPS, and use specific metrics for evaluating States' capabilities

The timely research, development, production, and distribution of certain critical vaccines and other medical supplies continue to be perplexing problems.[159] Vaccines and pharmaceuticals can cost hundreds of millions of dollars to develop, and little incentive exists for commercial manufacturers to produce pharmaceuticals with a potentially small or variable market. Moreover, private industry has become more risk-averse where vaccines are concerned because of the liability that they may incur. In addition, the Food and Drug Administration (FDA) must license vaccines and other pharmaceuticals after meetings standards for both safety and efficacy, which further delays their availability to the market. Human testing for efficacy is unethical, potentially unlawful, in the case of biological and chemical agents for which there is no known cure. FDA inspections are becoming increasingly stringent, making licensing even more challenging.

Recommendation: That DHHS, in collaboration with DHS and DoD, establish a national strategy for vaccine development for bioterrorism, which will be consistent with the nation's needs for other vaccines

The strategy may include tax incentives, liability protection, public-private initiatives such as the Government Owned Contractor Operated facility recommended in our previous report, and a guaranteed market.[160]

Implementing a Smallpox Vaccine

There has been significant debate on the nation's smallpox vaccination policy. This debate focuses on the uncertain level of threat of a smallpox attack and the certainty of adverse reactions to the smallpox vaccine. Recently, Federal health officials recommended a multiphase smallpox vaccination program for at risk emergency medical personnel with the Federal government assuming liability for adverse events related to vaccination. CDC sent a manual to all 50 States and Washington, DC in September 2002 with instructions on how to vaccinate entire populations within a week of an outbreak. The panel recognizes the significant accomplishment of acquiring sufficient doses of smallpox vaccine to immunize the population of the United States. The panel concurs with the evolving plan to voluntarily vaccinate limited numbers of healthcare providers and emergency responders.

Recommendations: That the smallpox vaccination plan be implemented in incremental stages with careful analysis and continuous assessment of the risks of the vaccine; and that DHHS place a high priority on research for a safer smallpox vaccine

---

[159] Wyeth announced that it would stop producing flu and pneumonia vaccines in 2002, leaving only one major producer. Recent experiences of the Department of Defense in the timely acquisition of reliable anthrax and adenovirus vaccines, as well as civilian shortages of influenza vaccines in 2000 and an ongoing tetanus toxoid shortage, highlight the magnitude of the problem. According to the American Society of Health System Pharmacists, supply problems for drug products have been increasing due to challenges in all segments of the supply chain: raw material sources, pharmaceutical manufacturers, federal regulators, wholesalers and other distributors, health care facilities, and pharmacies available at http://www.ashp.org/shortage/ accessed on October 12, 2001. In our second report, we noted that the TOPOFF exercise, conducted in May 2000, highlighted existing problems in the delivery and distribution of vaccines, antidotes, and prophylaxes. Unfortunately, as of the writing of this report, the Department of Justice has not yet released the TOPOFF After-Action Report, which was due in November 2000.

[160] At the time of the publication of this report, the enabling legislation for DHS contains liability protection issues for certain activities. Those provisions are, however, subject to modification when the new Congress convenes.

CHAPTER VII. DEFENDING AGAINST AGRICULTURAL TERRORISM

Agriculture and the food industry are critical to the economic, social and, arguably, political well being of the United States. One in eight people work in an occupation that is directly supported by the industry, which makes it the country's largest single employer. Cattle and dairy farmers alone earn between $50 billion and $54 billion a year through meat and milk sales,[161] while roughly $50 billion is raised every year through farm-related exports. In 2001, food production constituted 9.7 percent of the U.S. Gross Domestic Product (GDP), generating cash receipts in excess of $991 billion.[162] Agriculture's share of commodities sold overseas is also more than double that of other industries, which gives the sector major importance in terms of helping Washington's balance of trade.[163] Food imports valued at approximately $32 billion entered the market in 1998. Foreign sources accounted for 62 percent of fish, fish products and shellfish, 34 percent of fresh fruit, and 10 percent of fresh vegetables that Americans consumed in 1997.[164]

Although significant, these figures do not take into account allied industries and services, such as suppliers, transporters, distributors, and restaurant chains. According to the Department of Commerce (DoC), the economic multiplier effect of exported farm commodities alone is in the region of twenty to one.[165] The downstream effect of a major act of terrorism against this highly valuable industry would likely be enormous, impacting all of these sectors and ultimately, on the American consumer him/herself.[166] In addition, there is likely to be a major psychological impact on the producers, responders and the public more generally, and the psychological consequences of an act of agricultural terrorism are not well understood.

While there has been a focus in recent years in the United States on detecting, preventing and responding to terrorist threats and incidents, agriculture is one area that has received less attention. The antiterrorism focus, which has involved substantial financial outlays, has developed an increasingly well-protected public infrastructure in most sectors where, at a minimum, risk analyses have been used to expand contingency and consequence management responses to include terrorist incidents. In terms of accurate threat assessments and consequence management procedures, the agricultural sector continues to exist as an exception to the wide-ranging emphasis that has been given to infrastructure protection in this country in part because the sector was not included under the provisions of Presidential Decision Directive 63 (PDD-63),

[161] Overall livestock sales in 2001 were in excess of $108 billion. See "Agro-Terrorism Still a Credible Threat," *The Wall Street Journal*, December 26, 2001.
[162] Bureau of Economic Analysis, "Gross Domestic Product: First Quarter 2002 (Advance)," available at http://www.bea.doc.gov/bea/newsrel/gdp102a.htm.
[163] Shell, Ellen, "Could Mad Cow Disease Happen Here?" *The Atlantic Monthly*, 282/3, 1998, p. 92; "Stockgrowers Warned of Terrorism Threat," *The Chieftain*, August 19, 1999.
[164]Cohn, Jeffrey, "The International Flow of Food: FDA Takes on Growing Responsibilities for Imported Food Safety," U.S. Food and Drug Administration, *FDA Consumer Magazine*, January-February 2001 available at http://www.fda.gov/fdac/features/2001/101_food.html accessed October 31, 2002.
[165] Parker, "Agricultural Bioterrorism: A Federal Strategy to Meet the Threat" 11
[166] Wilson et al., "A Review of Agricultural Terrorism, Biological Crimes and Biological Warfare Targeting Animal Agriculture," p. 22.

which specified critical nodes deemed to be vulnerable to terrorist attack or disruption.[167] The current administration recognized agriculture and food as critical infrastructures that among other things "provide the essential goods and services Americans need to survive."[168] However, because agriculture and food have only recently been acknowledged as critical sectors, because terrorist threats against these infrastructures are uncommon, and because the *National Strategy* is focused on protection and not response, relatively little action has been taken to address the threat.

To address this shortcoming, the Advisory Panel is making a number of recommendations. These recommendations represent the beginning of a comprehensive strategy to address the threat of agriculture and food terrorism with a focus this year on agriculture. As the country begins to understand the scope and magnitude of the problem and begins to institute remedial measures, the panel is likely to have additional recommendations. It should be noted that, where appropriate, agriculture and food should be integrated into existing systems for planning, prevention, response, and information sharing. In addition, the dual use nature of some of these actions should be maximized. For instance, improved disease surveillance in animals will help to detect naturally occurring outbreaks as well as purposeful attacks, and food monitoring will prevent the spread of mistakenly contaminated as well as intentionally contaminated food.

Improving Resource Allocations

There has recently been recognition of the potential threat by the Congress and the Administration. President Bush proposed $146 million in new spending in FY03 to protect the nation's food supply from animal and plant pests and diseases, strengthen food safety programs, and support specific research activities. Several areas of funding relate to homeland security and the protection of agriculture:

- "$48 million increase for animal health monitoring to enhance the ability to quickly identify potential threats. These additional resources will be used to improve the emergency management system that coordinates and implements rapid response to an animal or plant pest or disease outbreak.
- "$19 million increase in the Agricultural Quarantine Inspection (AQI) program for improved point-of-entry inspection programs by providing additional inspectors, expanding canine teams and state-of-the-art high definition x-ray machines at high-risk ports of entry. This will bring staffing at ports of entry to 3,974.
- "$12 million increase for programs to expand diagnostic, response, management and other technical services within the Animal Plant Health Inspection Services (APHIS).

[167] In May 1998, the Clinton administration passed into law PDD-63 on Critical Infrastructure Protection. The initiative designates nine physical and cyber-based systems essential to the minimum operations of the economy and government that are deemed vulnerable to possible terrorist attack. Such sectors are taken to include: banking and finance; transportation; electricity, gas and oil; telecommunications; emergency law enforcement; government services; emergency fire; public health service; and the water supply. Agriculture and Food Safety is included as one of eight subgroups of the National Security Council's (NSC) Weapons of Mass Destruction Preparedness Group, which was established in 1998 under the auspices of Presidential Decision Directive 62 (PDD-62), "Combating Terrorism." See Henry Parker "Agricultural Bioterrorism: A Federal Strategy to Meet the Threat" McNair Paper 65, Institute for National Strategic Studies, National Defense University (March 2002), 30. For details on PDD-63 see White Paper, The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998.

[168] *National Strategy*, p, 30.

- "$28 million increase for the Food Safety and Inspection Service (FSIS). The increase will support FSIS food safety activities, including maintaining approximately 7,600 meat, poultry, and egg products inspectors. This funding would include $14.5 million to improve the information technology infrastructure to improve risk management systems and $2.7 million for slaughter epidemiological surveys and risk prevention activities.
- "$34 million increase to support research aimed at protecting the nation's agriculture and food system from attack by animal and plant diseases, insects, and other pests and to reduce the incidence of food-borne illness in humans due to pathogens and other threats to the food supply. These increases will emphasize development of improved detection, identification, diagnostic, and vaccination methods to identify and control threats to animal and plant agriculture.
- "$5 million increase to strengthen the capability of APHIS to assess and monitor outbreaks of diseases in foreign countries that have the potential to spread to the United States."

In addition, appropriations for 2002 provided an additional $328 million in USDA funding for homeland security related protections. This includes $105 million for APHIS pest and disease exclusion, detection, and monitoring; $80 million for upgrading USDA facilities and operational security; $50 million for an animal bio-containment facility at the National Animal Disease Laboratory; $40 million for the Agricultural Research Service; $23 million for the Plum Island Animal Disease Center; $15 million for security upgrades and bioterrorism protection for the FSIS; and $14 million for increased security measures at the National Veterinary Services Laboratories in Ames, Iowa.[169]

Understanding the Threat

As noted in the updated threat assessment earlier in this report, the threat to agriculture has received relatively little attention in the national security arena and from State, local, and private sector entities involved in this critical infrastructure. For a variety of reasons, the U.S. agricultural sector remains acutely vulnerable to attack. Critical susceptibilities stem from six main factors:

- The concentrated and intensive nature of contemporary U.S. farming practices;
- The increased disease susceptibility of livestock;
- A general lack of farm/food-related security and surveillance;
- An inefficient passive disease reporting system further hampered by a lack of trust between regulators and producers;
- Veterinarian training that tends not to emphasize foreign animal diseases (FADs) or large-scale husbandry; and
- A prevailing focus on aggregate, rather than individual animal statistics.

During the past administration, the industry was not recognized in the nation's efforts to protect critical infrastructure and was not included under the provisions of PDD-63. Agriculture and Food Safety is included as one of eight sub-groups of the National Security Council's (NSC) Weapons of Mass Destruction Preparedness Group, which was established in 1998 under PDD-

[169] Release No. 0026.02 Alisa Harrison "President's Budget To Provide $146 Million Increase in Funding to Protect Agriculture and the Nation's Food Supply," USDA News Release available at http://www.usda.gov/news/releases/2002/01/0026.htm, accessed on November 6, 2002.

62, "Combating Terrorism." The USDA serves as chair of this subgroup. However, the USDA lacks sufficient visibility and influence to champion greater Federal attention to countering biological attacks against agriculture.

The USDA's Office of Crisis Planning and Management (OCPM) is responsible for coordinating USDA's requirements to the Intelligence Community and sharing intelligence information among USDA offices and agencies.[170] However, an overarching appreciation of the true threat to America's agriculture is lacking. Without a broad threat assessment it is difficult to prioritize resources to counter the terrorist threat.

Recommendation: That the President direct that the National Intelligence Council, in coordination with DHS, USDA and DHHS, perform a National Intelligence Estimate on the potential terrorist threat to agriculture and food

Enhancing Planning

As with other disasters and emergencies, the response to an act of agricultural terrorism would require participation by numerous local, State, and Federal agencies, as well as industry and other private organizations. The response should be coordinated through the emergency management system. The Animal Health Emergency Preparedness Plan, developed by the National Emergency Management Association with funds from the USDA provides a guide for comprehensive emergency management plans for the response to emergencies involving animals and the animal industry segment of production agriculture, and as a source of information on national trends for States already having such plans. The plan is designed for inclusion in State Emergency Operations Plans. It builds on existing concepts of operation and mutual aid agreements.[171] The Emergency Support Function (ESF) in the Animal Health Emergency Preparedness Plan is not currently applicable to any ESF in the Federal Response Plan. Therefore the State agency or agencies with statutory authority will be responsible for the function.

Recommendation: That the Assistant to the President for Homeland Security ensure that an Emergency Support Function for Agriculture and Food, consistent with the intent of the ESF described in the Animal Health Emergency Preparedness Plan, be included in the Federal Response Plan and the National Incident Response Plan under development

There are many critical aspects to such a plan. These include understanding who is in charge; the laws and authorities governing response; information sharing among those involved including all levels of government and the private sector; a comprehensive communication strategy for the public and including the media, which takes into account the psychological dimension of the threat; and response capabilities. Each of these is discussed in some detail below.

---

[170] "National Security: U.S. Department of Agriculture," available at http://www.usda.gov/da/ocpm/security.htm, accessed on November 6, 2002.

[171] NEMA, Model Emergency Support Function for Production Agriculture, Animal, and Animal Industry," September 2002, available at http://www.nemaweb.org/library/documents/Model_Plan_for_Animal_ESF.pdf.

The *National Strategy for Homeland Security* specifies that infrastructure protection will be integrated and coordinated in the Department of Homeland Security with the Department of Agriculture acting as the lead agency with the primary responsibility for interacting with the agriculture and meat and poultry sectors. The Department of Health and Human Services will be the lead agency for all other food products. Other agencies involved in protecting agriculture and food include the U.S. Departments of State and Commerce, the Environmental Protection Agency, and the Office of the U.S. Trade Representative. States also play a significant role. This plethora of interests may make it difficult to respond efficiently to an attack on America's agriculture or food.

Currently, as with bioterrorism, it is unclear who is in charge in the event of an agricultural attack at the Federal level. Several agencies are involved in different parts of the agriculture chain. As examples:

- FSIS regulates meat, poultry, and egg products, which account for thirty percent of consumer spending for food, with an annual retail value of $120 billion. FSIS maintains a system of import inspection and controls. Also, FSIS annually "reviews inspection systems in all foreign countries eligible to export meat and poultry to the United States to ensure that they are equivalent to those under U.S. laws."[172]
- The FDA monitors all food sold in interstate commerce, including shell eggs but not meat and poultry, bottled water, and wine beverages with less than seven percent alcohol.
- The CDC investigates with local, State, and other Federal officials sources of food-borne disease outbreaks and maintains a nationwide system of food-borne disease surveillance.
- The National Oceanic and Atmospheric Administration inspects and certifies fishing vessels, seafood processing plants, and retail facilities for Federal sanitation standards.
- The U.S. Marshals Service seizes unsafe food products not yet in the marketplace, as ordered by courts.[173]
- The U.S. Customs Service works with Federal regulatory agencies to ensure that all goods entering and exiting the United States do so according to U.S. laws and regulations.

While clearly much of the agricultural and food products that cross State and international boundaries are subject to inspection, FDA and USDA do not have the resources to inspect all of the food entering the United States. Therefore, these organizations must coordinate with those who export food to America to ensure the safety of American citizens. One vehicle for cooperation is the Codex Alimentarius Commission, run by the World Health Organization (WHO) and the Food and Agricultural Organization (FAO). Codex's 165 member countries establish international standards for agricultural products and food commodities and set safety standards for food additives and contaminants and for veterinary drugs.[174]

The lack of clarity in the responsibility for agriculture and food safety may create confusion in the event of an attack on agriculture or processed food. Reflecting the mandate in the *National Strategy for Homeland Security*, if an attack of agricultural terrorism occurred in the United

[172] FSIS Backgrounders, "Protecting the Public from Foodborne Illness: The Food Safety and Inspection Service, April 2001, available at http://www.fsis.usda.gov/oa/background/fsisgeneral.htm, accessed on November 6, 2002.
[173] U. S. Food and Drug Administration, FDA Backgrounder, "Food Safety: A Team Approach," September 24, 1998 available at http://vm.cfsan.fda.gov/~lrd/foodteam.html, accessed on November 6, 2002.
[174] Ibid.

States, DHS should be the lead agency and USDA should be the principal supporting agency for a newly developed Emergency Support Function in the developing National Incident Response Plan. As such the USDA should coordinate with FDA, Customs, Commerce, and others and with State emergency management agencies and other State, local and private responders. As with other emergency functions this response function should be included in interdisciplinary terrorism response exercises.

The legal and regulatory regime must be clear when developing a plan to respond to an act of terrorism. The Model State Emergency Health Powers Act, written by Lawrence Gostin, provides a blueprint for State legislation that gives governors and State health officials the authority to enforce quarantines, vaccinate people, seize and destroy property without compensation, and ration medical supplies, food, and fuel in a public health emergency. It has been adopted by a number of States; however, there is no comparable legislation for authorities to respond to an agricultural attack. To standardize laws and authorities across the country the USDA should commission a Model State Agricultural Disease Emergency Security Act in consultation with State authorities.

DHHS has supported efforts to better connect emergency management, public health, law enforcement, and other entities involved in combating terrorism through such initiatives as the Health Alert Network (HAN). The agricultural community is not well integrated into this and other systems. In fact, many veterinarians are not connected to the Internet. As part of the emergency response plan described above, the USDA, DHHS, and DHS should work to include the agricultural community in all developing communications strategies.

For many animal diseases, vaccines and treatments exist that can limit the spread and scope of an attack; however, for foreign animal diseases, the stockpiles in the United States either do not exist or the numbers are inadequate. As part of the agricultural response plan, the USDA, in consultation with DHHS, should store vaccines, pesticides, herbicides, and other needed equipment and supplies as a component of the National Pharmaceutical Stockpile." These supplies would be available for response to a large-scale outbreak. To decide on the components of the Stockpile, the USDA, in consultation with other relevant Federal, State, and local officials, and the private sector should undertake a study to understand current stores of needed pharmaceuticals and supplies and assess shortcomings based on a risk assessment for the agriculture and food sector.

The United States has not faced a mass disease outbreak in the agricultural sector in the recent past. It is unclear the psychological impacts of such an attack and such a response as a mass culling operation. Individuals affected by the FMD outbreak in the United Kingdom experienced a range of psychological symptoms. The results of a survey in Great Britain showed that those seeking assistance commonly experienced tearfulness, lack of sleep, loss of appetite, increased consumption of alcohol and tobacco, increased anger, irritability, increased marital and domestic discord, and general feelings of depression. Health practitioners also reported seeing farmers and business owners with a range of mental health problems from stress, anxiety, and depression.[175] To minimize the psychological impact, as part of the agricultural response plan,

[175] Deaville J, Jones L. The Health Impact of the Foot and Mouth Situation on People in Wales—The Service Providers Perspective. A summary report to the National Assembly for Wales by the Institute for Rural Health. May 2001.

the USDA in concert with DHS, DHHS, and State and local officials should develop a public communications strategy for before, during, and after an attack that takes into account the potential psychological impacts of an agricultural attack.

The American veterinary community is only partially integrated into Federal disaster response systems. In 1993, the American Veterinary Medical Association (AVMA) became part of the National Disaster Medical System (NDMS). Veterinary health professionals are organized into Veterinary Medical Assistance Teams (VMAT), which respond to the needs of animals during disasters. In 1994, the VMAT role was expanded to assist the USDA in the "control, treatment, and eradication of animal disease outbreaks." The veterinarians, technicians, and support personnel provide assistance if the local veterinary community is overwhelmed. Deployment is meant to occur to any State or United States territory within 24 – 48 hours when the State officials from the affected State request their assistance. The members can sustain themselves for three days. Team members are preprocessed for Federal employment and issued identification cards. These persons can then be called to Federal service for up to 14 days as "special needs" employees of the U.S. Public Health Service and as such are protected under the Federal Tort Claims Act against personal liability and are exempt from licensure, certification, or registration requirements. The AVMA and American Veterinary Medical Foundation (AVMF) were recognized in 1998 as the only national organizations representing licensed veterinarians and are solely responsible for the care of animals, including during periods designated as disaster relief. These organizations should be carefully integrated into the ESF in the National Incident Response Plan and also into planning by State and local officials.

As with other parts of the economy, the agricultural system has moved to "just in time" logistics, but the disease surveillance system has not kept pace. Animals in the United States travel long distances during their lifetime and tracking mechanisms are insufficient. For instance, a pound of meat generally travels about 1,000 miles on the hoof before it reaches the dinner table. Between 20 and 30 percent of cattle were regularly consigned to non-slaughter destinations at least 25 miles from their original point of purchase and in many cases had crossed several States within 36 to 48 hours of leaving the sales yard. To enable rapid response to an act of terrorism against agriculture or a natural outbreak, tracking products from the breeder to the table is critical. This will involve both government and private sector personnel and resources.

Improving Laboratory Capacity

There are only two existing civilian biosafety level 4 (BSL 4) laboratories for working with and diagnosing the most hazardous animal pathogens, the National Veterinary Services Laboratories in Ames, Iowa, and Plum Island, New York. Infectious animal diseases can only be studied and Foot and Mouth Disease testing is only allowed at Plum Island by law.[176] Samples must be shipped to this location for testing, wasting precious time before the diagnosis of an outbreak. To minimize the impact of any outbreak it is critical that laboratory tests be performed quickly. Having to send samples across the country (if an outbreak occurred in California) might delay appropriate responses. Recognizing this, Ken Foster, professor of agricultural economics at Purdue University noted, "If some state diagnostic labs were allowed to test for FMD, that would

[176] Plum Island Foreign Animal Disease Laboratory available at http://www.globalsecurity.org/wmd/facility/plum_island.htm on November 11, 2002.

reduce the time it takes to make the diagnosis."[177] The Armed Forces Institute of Pathology (AFIP), Department of Veterinary Pathology, can also assist in identifying and diagnosing animals' diseases. If an outbreak of a foreign animal disease occurs in the United States, early detection will be critical in the containment and elimination of disease. These would provide insufficient capacity in the event of a large-scale outbreak. Probabilities suggest that by the time an outbreak is detected, it will have already spread to more than one location, probably in more than one State. Capabilities at the State level would increase the ability to detect foreign animal diseases early. A pilot program currently tests for eight animal diseases including foot and mouth disease, hog cholera, and others at the State level.[178]

Recommendation: That the President propose and that the Congress enact statutory provisions for the certification under rigid standards of additional laboratories to test for Foot and Mouth Disease and other highly dangerous animal pathogens

At the end of 2001, the U.S. Animal Health Association (USAHA) passed a resolution recommending that the Department of Agriculture enable State veterinary laboratories to perform tests and increase surveillance for foreign agricultural diseases.[179] In its response to USAHA, USDA said that "(l)aboratory test results can be ready within between eight hours to several days after receipt of samples" and that "(i)n an outbreak situation, where laboratory diagnosis would overwhelm Federal capacity, consideration to allow State diagnostic laboratories to test would be given." But without advance training and the appropriate equipment and security in place prior to an outbreak, it is not likely that State labs will be adequately prepared to respond to a crisis. With the creation of the Department of Homeland Security, that department will now have certain specific authority in this area.

Recommendation: That the Secretaries of Homeland Security and Agriculture (consistent with the November 2001 resolution of the United States Animal Health Association) jointly publish regulations implementing a program to train, equip, and support specially designated, equipped, secure, and geographically distributed veterinary diagnostic laboratories to perform tests and enhance surveillance for agricultural diseases that are foreign to the United States

Compensating for Agricultural Losses

The United States does not have a national, standardized system of compensation in place for reimbursement to producers for losses stemming from an agricultural disease outbreak. This lack of clarity may prevent producers, and others in the agricultural community from coming forward when they suspect infected animals or food. Otto Doering, professor of agriculture at Purdue University, recommends that the USDA distribute a decisive statement alerting producers that if FMD were found in their herds, they would receive adequate reimbursement for any

[177] Purdue News Service, "Purdue experts propose ideas to deal with foot-and-mouth disease," April 13, 2001 available at http://news.uns.purdue.edu/UNS/html3month/010413.Doering.fmd.html accessed on November 11, 2002.
[178] Powell, Charlie, " WSU Animal Disease Diagnostic Laboratory Awarded $750,000 for Homeland Security," News @ WSU, August 30, 2002 available at http://www.wsunews.wsu.edu/detail.asp?StoryID=3234, accessed on November 29, 2002.
[179] See Appendix G.

animals destroyed. "Such things as larger payments for breeding stock need to be made clear so as to encourage farmers to come forward if there is an outbreak," Doering said.[180] USDA provides compensation on a case-by-case basis. To encourage reporting of diseases and to ensure the stability of the agricultural sector, it is critical that a consistent scheme of national compensation be in place to provide financial assistance to producers and other agribusiness interests affected by an animal disease outbreak.

Recommendation: That the Secretary of Agriculture, in consultation with State and local governments and the private sector, institute a standard system for fair compensation for agriculture and food losses following an agroterrorism attack; and that the Secretary of Health and Human Services should develop a parallel system for non-meat or poultry food

The Animal and Plant Health Inspection Service (APHIS) recently published a proposed rule, "Foot-and-Mouth Disease Payment of Indemnity," on May 1, 2002,[181] that changes indemnity requirements primarily related to FMD. This rule would make the compensation of producers more fair and transparent and enhance the likelihood that they would come forward to report potential infections. This rule should be broadened to encompass all diseases that threaten livestock. Once a compensation plan is in place, the USDA along with State and local officials should develop an information dissemination strategy so that those involved will be well informed. In addition, incentives for disease reporting at all facilities and levels should be provided.

Promoting Better Education and Training

While some States are preparing for the threat of agricultural terrorism, others have not begun to establish the information sharing channels, plans, and structures to adequately address the threat. A number of different persons or entities at the State level are in charge of the public agricultural sector for the State including lieutenant governors and State cabinet level officials. These and other State and local officials need to be educated on the threat and need to open communication lines with State, local, and Federal law enforcement officials and the Intelligence Community.

At another level, there is a lack of expertise and sheer numbers of personnel available to work to secure the U.S. agricultural infrastructure. Not enough appropriately trained veterinarians are capable of recognizing and treating exotic livestock diseases in the United States because fewer people are entering veterinary science, reflecting the lack of educational support and financial incentive given to the discipline in the country and because most veterinarians focus on domesticated pets rather than large-scale husbandry. Veterinary degree curricula should include courses on foreign animal diseases. The need for more large-animal veterinarians was recognized in a recent conference entitled "Food Animal Veterinarians: An Endangered Species."[182] According to the American Veterinary Medical Association, which represents

[180] Purdue News Service, "Purdue experts propose ideas to deal with foot-and-mouth disease," April 13, 2001 available at http://news.uns.purdue.edu/UNS/html3month/010413.Doering.fmd.html accessed on November 11, 2002.
[181] Federal Register (67 FR 21934-21959, Docket No. 01-069-1).
[182] Held at Kansas State University's College of Veterinary Medicine, October 25-26, 2002 available at http://www.fass.org/fasstrack/news_item.asp?news_id=745, accessed on November 6, 2002

82 percent of veterinarians in the United States, only 751 veterinarians declare themselves as bovine exclusive with another 3,000 declared as "mixed large animal" veterinarians.[183]

In addition, college curricula do not emphasize foreign animal diseases, with most focus on diseases endemic to the United States. Therefore, a dearth of accredited State and local veterinarians have either a background in farm animal diagnostics or the necessary expertise to deal with "Class A" agents.

Other types of expertise required for dealing with agricultural diseases are lacking. For instance, entomology expertise is shrinking, presenting difficulties for understanding vectors and response.[184] In addition, government compensation in laboratories is weak compared to the private sector, making it difficult to attract experienced personnel. This leaves the agricultural sector ill-equipped to recognize and respond to a manmade or naturally occurring attack against agriculture.

Recommendation: That the Secretary of Agriculture develop and that the Congress fund programs to improve higher education in veterinary medicine to include focused training on intentional attacks, and to provide additional incentives for professional tracks in that discipline

That the Secretary of Agriculture, in coordination with States, improve education, training, and exercises between government and the agricultural private sector, for better understanding the agroterrorism threat, and for the identification and treatment of intentional introduction of animal diseases and other agricultural attacks

[183] Author interview, October 31, 2002

[184] For instance the article by W. C. Reeves. "Concerns About the Future of Medical Entomology in Tropical Medicine Research," Am. J. Trop. Med. Hyg. 1989, 40:569-570, laments the shortage of medical entomologists and "Growing Pest Control Industry Faces A Shortage Of Entomologists," Wendy McDowell, UF/IFAS Educational Media & Services, (352) 392-2411, Sources: Phil Koehler, (352) 392-2484; Bruce McCown, (352) 376-2661, Feb. 18, 1997.

CHAPTER VIII. IMPROVING THE PROTECTION OF OUR CRITICAL INFRASTRUCTURE

In our previous reports, we have focused our attention in the area of critical infrastructure protection (CIP) on matters of cyber security. The cyber piece of the CIP effort continues to be, in our view, the most problematic and challenging in that arena. Much work has been done to enhance the physical protection of certain critical infrastructures, but more remains to be accomplished. Little real success has been achieved in the cyber realm, perhaps because of its complexities or perhaps because its imperatives are less well understood.

In our *Third Report*, we recommended that "the Congress create an independent commission, tasked to evaluate programs designed to promote cyber security, to identify areas where requirements are not being met, to recommend strategies for better security, and to report its findings to the President and the Congress." That recommendation has not yet received favorable consideration by the Congress. Later in this chapter, we will restate and expand that recommendation to include all aspects of CIP, with a comprehensive framework for the types of issues that should be comprehensively addressed by that commission.

We have concluded that the physical and cyber elements of CIP are so intertwined that it makes no sense to address them separately. We will also make additional recommendations for improving CIP that need to be addressed on an urgent basis, regardless of whether a new commission is established.

First, some discourse on the current nature of the CIP problem is in order.

Reconciling Definitional Terms

"Critical infrastructure" can mean different things to different people. But it is important that everyone has a common baseline of definitions or terms, so we are not talking past each other. Neither the Administration's proposed legislation for establishing the Department of Homeland Security nor the Bill as passed define the term; nor does the *National Strategy*.

There is a useful definition, at least, in the 1997 report of the President's Commission on Critical Infrastructure Protection:[185]

> *Infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security.*

That definition, or something like it, should be adopted by all policymakers.[186]

---

[185] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure*, October 1997.

[186] In response to the Commission's report, President Clinton signed Presidential Decision Directive Number 63 (PDD-63) on May 22, 1998. The Directive defined critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government." That, in our view, falls well short of a comprehensive and comprehensible definition. A more comprehensive definition is contained in Section 4. (2), S. 1456 Critical Infrastructure Information Security Act of 2001 (Introduced in the Senate); September 24, 2001: "The term 'critical infrastructure'--

The *National Strategy* the following as the "Critical Infrastructure Sectors:

- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Government
- Defense Industrial Base
- Information and Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry
- Postal and Shipping

Interestingly, the *Strategy* does not list "hospitals and other medical care providers;" that system is different from "public health," especially since most of it belongs to the private sector; not all medical care is an emergency service. Nor does it list "law enforcement" unless that sector is subsumed in emergency services; of course, not all law enforcement is an emergency service.

More importantly, many in government and the private sector do not make the necessary distinction between "critical infrastructure protection"—often abbreviated "CIP"—and "critical information infrastructure protection"—sometimes called CIIP, or perhaps more appropriately "cyber security."[187] CIIP or cyber security challenges permeate all CIP sectors and, indeed, now most every aspect of American life.

Enhancing Resources and Establishing Appropriate Burden Sharing

In the weeks and months following September 11, 2001, State and local governments and private sector entities responded to the increased threat to the nation by taking measures to safeguard their critical infrastructures and protect their populations and workforces. These additional costs were necessary but burdensome, and these actors looked forward to fiscal support for reimbursement and other resources that they believed had been promised by the Federal

---

"(A) means physical and cyber-based systems and services essential to the national defense, government, or economy of the United States, including systems essential for telecommunications (including voice and data transmission and the Internet), electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services (including medical, fire, and police services), and the continuity of government operations; and

"(B) includes any industry sector designated by the President pursuant to the National Security Act of 1947 (50 U.S.C. 401 et seq.) or the Defense Production Act of 1950 (50 U.S.C. App. 2061 et seq.) as essential to provide resources for the execution of the national security strategy of the United States, including emergency preparedness activities pursuant to title VI of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5195 et seq.)."

[187] The terms are, unfortunately, often used synonymously or interchangeably. See testimony of John Tritak, Director, Critical Infrastructure Assurance Office, before the Senate Judiciary Committee Subcommittee on Technology, Terrorism and Government Information, October 6, 1999.

government. Much of these funds have not yet found their way to the intended recipients. In the case of State and local governments, this is a particularly onerous, because many State constitutions require a balanced budget. In these States in particular, but to some degree in almost every jurisdiction, other services have been cut to pay for increased security. This problem is exacerbated by the continuously elevated threat level (yellow), recurring periods of heightened alert (orange level), and targeted warnings for specific regions of the country or designated critical infrastructures.

That does not suggest that such warnings are not well intentioned or necessary; they are. While the concerns that led to the warnings have not resulted in any more attacks, the burden these warnings place on both public and private sector organizations charged with security missions have been significant. That situation has been further complicated by the absence of any set of substantive actions that should be undertaken by an entity when a warning is received.

This fundamental issue—homeland security burden sharing—deserves far more formal attention.[188] While the September 2001 attacks made the importance of homeland security starkly clear, it did not help define who should pay for what, and what measures give the greatest return on investment remains unclear. This is one of the fundamental public policy issues of the next decade, and one that will significantly affect such critical issues as the provision of homeland security and national defense, the maintenance of social well being, and the health and viability of U.S. commercial interests. The second of these is a first-order question that requires innovative thinking and solid economic analysis and a question that we believe can only be answered by a body of experts, sufficiently sheltered from the dynamics of the political process to permit it to conduct objective research and analysis.

Improving Information Sharing

The homeland security legal framework is relatively new and still developing. Many critical issues are being addressed by the Administration, the Congress, and State and local governments. One area of importance that crosses several boundaries, and one especially important in the context of CIP—especially cyber security—is information shared by private sector organizations with the Federal government. This can expose corporations to liability concerns as well as the potential for inadvertent disclosure of proprietary or other sensitive information.

There are provisions in the enabling legislation of the new Department of Homeland Security that provide certain protections for critical information provided *voluntarily* to the government by private sector entities.[189] That is an important step. It is reasonable to assume that, if such provisions are not deemed satisfactory by the government in terms of the quality or quantity of information provided, future legal or regulatory regimes may *demand* some types of information.

On the one hand, requiring that security related information be provided would force the private sector to implement better security practices to avoid liability, while on the other, failing to provide some liability protection would all but ensure that the private sector will not share

[188] Burden sharing implies the questions of public vs. private, and federal vs. State vs. local.
[189] Subtitle B, "Critical Infrastructure Information," Pub. L. 107-296 (H.R. 5005, 107th Congress, 2nd Session), November 25, 2002, reproduced at Appendix M.

potentially critical information. This continues to create a conundrum for private entities and the government.[190]

Determining Appropriate Identification and Access Control

The argument for a homeland security identification system for government employees performing critical or sensitive functions is not difficult to make. Indeed, all federal agencies currently have some form of identification system. More problematic is the concept of an identification system for private citizens who handle sensitive information or dangerous substances or otherwise perform functions critical to public health and safety. Examples of positions for which such a system might be desired range from the operators of nuclear power plants, to airline baggage handlers and drivers of HAZMAT trucks. Some of these positions will require nothing more than the ability to positively verify the identity of the person seeking access to a facility or information, while others may require some background checks or other information.

Concerns about privacy and misuse of personal data on the part of the government are prudent, and care must be exercised in examining the wisdom of such a system. Nonetheless, we feel that circumstances warrant examining the implications of such a system for certain jobs, as the implications for our collective security and individual health and safety are grave. Furthermore, any such system must be national in character if it is to be truly effective and may need to mesh with a future government identification system. However, meticulous care should be exercised in identifying what positions should be included in this scheme, what private information should be maintained on the holders of these positions, who should have access to that information, and how that information should protected. All stakeholders must have their concerns considered, and have some form of representation in the deliberations on creating such a system.

Improving the Roles of the Public At Large

One component of the homeland security effort that has not gotten enough attention has been the role of the public as a critical component of the solution—indeed, as a critical infrastructure in and of itself. The Terrorism Information and Prevention System, generally referred to as Operation TIPS, was first introduced by President Bush as part of the USA Freedom Corps program in the January 2002 State of the Union address. It was envisioned as a voluntary reporting system to "enable American workers to report unusual and non-emergency issues that they observe in the normal course of their work."[191] Mail carriers, utility employees, truckers, and other workers were encouraged to report suspicious and potentially terrorist-related activity to the Operation TIPS website or telephone hotline, where it would be entered into a national database. However, the program came under intense opposition from Federal lawmakers, the American Civil Liberties Union (ACLU), and such government agencies as the U. S. Postal Service. The major concern was that it would infringe on the privacy rights of American citizens by encouraging millions of workers with access to private homes to spy on customers. As Rachel King, legislative counsel of the ACLU, argued, "The administration apparently wants to implement a program that will turn local cable or gas or electrical technicians into government-

[190] For a recent, excellent commentary on the nature of this problem, see the statement of Senator Robert Bennett, C*ongressional Record,* November 19, 2002, pp. S11562-S11563, reproduced at Appendix N.
[191] Statement of Barbara Comstock, Director of Public Affairs, Department of Justice, July 16, 2002.

sanctioned peeping toms."[192] Indeed, the Homeland Security Act of 2002 (H.R. 5005) included language that explicitly prohibited Operation TIPS from being implemented.

Despite the failed attempt of the TIPS program, there are tangible functions and responsibilities the public can and should take on, such as awareness of food and water safety issues, which do not which do not carry negative connotations.

But this issue is larger than that. In fact, "we should recognize that the government, alone, cannot always protect us from terrorists. Catching small, covert terror cells is not unlike catching spies—both seek to hide in and use our open society and the resources of our nation against us, and succeed by evading the government agencies established to protect society. History teaches that some will evade government detection."[193]

This topic is controversial on several levels. First, our very social fabric is founded on individual freedoms, and creating a situation in which neighbors spy on each other would not only be undesirable but almost certainly counterproductive. Furthermore, constructive involvement by the public would entail a significant education and training effort to make the general public aware of signs of terror (e.g., behavior patterns, suspicious materials, practices defined in terrorist training manuals) and not interpret religion, ancestry, or culture as terrorist indicators. Finally, a real reliance on public participation would involve a shift from a law enforcement/defense metaphor for homeland and national security, in which the government is responsible for our collective security, to a "wagon train" metaphor in which each member of society bears some responsible for the collective security of the whole. That said, little hard analysis of this absolutely critical issue exists.

Enhancing Cyber Security

National coordination of cyber security policy has not significantly improved. The President's Critical Infrastructure Protection Board (PCIPB) has not had a large affect on policymaking, apparently relying, instead, on the White House Office of Cyberspace Security. The *Draft National Strategy to Secure Cyberspace* presents a clear example. This document, introduced by a cover letter from the Chair and Vice Chair of the PCIPB, apparently has not been cleared by the full Board despite the appearance to the contrary in the introductory letter. Furthermore, the new governmental structure designated by Executive Order 13231 is in fact only marginally different than that put in place four years earlier by PDD 63. Moreover, recommendations in our earlier reports that key State and local government and private sector representatives be included on key policymaking entities, such as this Board, have not been acted upon.

In addition, the *Draft National Strategy to Secure Cyberspace* attempts to straddle the intellectual and policy gap represented by the power of the government to mandate certain actions that would have a salutary affect on the security of cyberspace with the tacit recognition that entrepreneurial forces are more efficient than government mandates. As a result, it continues and extends the policies in place for the past several years that rely on "public-private

[192] Stacy Humes-Schulz, "Alarm Bells Ring Over Terrorism Reporting System," Financial Times, July 23, 2002, p. 6.
[193] Terrence K. Kelly, "Vigilance is our Civic Duty", *Pittsburgh Post Gazette,* September 11, 2002*,* available at http://www.post-gazette.com/forum/comm/20020911edterr11p4.asp.

partnerships"—meaning that it relies on private sector willingness to take certain security measures and bear their costs and chooses not to use government's power to legislate, regulate, or otherwise require certain actions. As a result, the *Draft Strategy* poses what we view as voluntary, tactical responses to an inherently strategic problem of national importance. If it is adopted, it will be a step in the right direction but a small step indeed.

As we stated in our report last year, "This is an exceptionally complex topic, one that spans national security, law enforcement, civil [liberties], and commercial and other private-sector interests."[194] If anything, cyber security, its importance, and the issue of who should bear the burden for providing it will increase in complexity and difficulty with the increasing complexity of the networks. It is our firm belief that the single most important step in developing good public policy for cyber security, and a step that is notably immature, is to develop an understanding of the problem. Other key background areas are an outline of the government approach to the problem, and private sector trends and concerns.

Earlier in this chapter we highlighted some concepts and analyses that must be undertaken, and which are critical to furthering our understanding of the general homeland security problem and development of cogent policy. But policy decisions by the Federal government are also hindering this maturation process. Key problems in the approach to date are defined by the following characteristics:

- Cyber security has been isolated and specialized, thus limiting its perceived relevance to day-to-day outcomes and even its relevance to what are viewed as clear and present homeland security threats.
- Creating a separate strategy and Executive Branch organizational structure for cyber and physical security has reinforced the isolated and add-on nature of cyber security to such an extent that it has drawn criticism from the private sector as burdensome bureaucratic layering, thereby significantly detracting from its relevance.
- In focusing on the need for public-private partnership so intensely, the government has failed to recognize the fundamental importance of market factors and largely failed to exercise any of its powers besides persuasion. As a result, there has been no change in the significant market disincentives to the adoption of cyber security measures necessary for ensuring the viability of critical functions performed by the information infrastructure that directly contribute to national needs (e.g., national security, public health, and safety).
- Applying this same standard to the public sector has produced the result that no one is clearly responsible for the security of information infrastructure "commons" or held accountable for cyber security lapses. The Federal government does not hold its leaders and managers responsible for cyber security. There are essentially little or no consequences for Federal government agencies and officials who do not take prudent steps to improve cyber security.

[194] *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction,* p. 41.

Accounting for Private Sector Concerns

The concerns expressed to us by key critical infrastructure stakeholders in the private sector are in certain respects divergent, but common themes exist. In general, extensive interviews conducted by supporting staff at RAND with representatives of key stakeholders indicate that

- The vast majority of security failures stem from poorly configured systems and workforce training issues, and are caused in part by poorly written software and the inability to understand the security implications of the increasingly complicated systems of systems that is the information infrastructure.
- Corporations are in the business of managing risk, of which cyber security risk is just one. If better risk models make clear that good cyber security is of greater value than previously acknowledged, businesses will invest in more of it.
- Rapidly changing technology, most prevalently in the form of mobile networks and embedded computing and communications devices, are likely to make the cyber security situation much worse if certain fundamental steps are not taken (e.g., establishment of security standards and improvements in software and hardware security engineering).
- Key reforms cannot be accomplished without fundamental changes in the information technology market that significantly increases the understanding of importance of cyber security.
- Mechanisms that could increase the market value of security include
  – statutes and regulation that require certain specified levels of security;
  – changes in insurance and auditing practices that reward good security practices;
  – increases in the availability of secure products and services brought about, for example, by demand from very large customers (e.g., the Federal government) and that significantly lower the cost of adopting more secure systems and practices by smaller customers and users; and
  – changes in liability law that assigns responsibility for security in both the enterprise and information infrastructure commons and limits the externalizing of cyber security risk.

The Need for an Independent Commission

Recommendation: That the Congress establish and that the President support an Independent Commission to suggest strategies for the protection of the nation's critical infrastructures

The importance of such an Independent Commission is hard to overstate. This new area contains many very sensitive issues of great importance about which objective research and proposals are very difficult to conduct and develop within the political process. It is also important to realize that recommendations for resolving these issues cannot be based on the current make up of either the Executive or Legislative Branches of the Federal government and that issues requiring action by one branch or level of government (i.e., Federal, State and local governments) or the private sector, alone, do not in general require the special level of attention that makes an Independent Commission necessary. General categories of issues that might be appropriate for the Independent Commission include those that span different national equities—i.e., require actions by or changes in both the Executive and Legislative Branches of government; actions by or changes in multiple levels of government; government intervention in the conduct of private sector entities, and the internal and external relationships of entities in the private sector.

In line with our previous discussion of the central issues in critical infrastructure protection, it is our opinion that an Independent Commission must, at a minimum comprehensively address the following:

- **Burden sharing between public and private sector organizations responsible for homeland security, and among Federal, State and local governments, including basic principles and guidelines for these determinations. Such policies should be based on analysis of the effectiveness and efficiency of different types of programs and potential solutions.**
- **Liability protection for corporations that share information with the Federal government, taking into account compulsory and voluntary sharing considerations.**
- **The need for and impact of an identification system for private sector positions that have significant homeland security implications, including guidelines for such a system.**
- **Public participation in homeland security, including areas, if any, in which the government must have help from the public, how best to develop this capability, and the implications for civil liberties and effects on our culture.**
- **Critical social functions impossible to sustain without the information infrastructure, including options that would compel their security (e.g., regulations or statutes governing their security itself, audit standards or insurance provisions, and changes to liability laws that would place a reasonable share of the security burden on product/service providers).**
- **Information infrastructure "commons" and assigning responsibility for their security to appropriate public or private sector organizations or communities.**
- **In coordination with the President's National Infrastructure Advisory Council, National Security Telecommunications Advisory Committee, and the President's Committee of Advisors on Science and Technology and supported by comprehensive, expert economic analysis, examine the information technology market mechanisms to determine the information security market structure and competitiveness issues and make recommendations for changes that would accomplish the security goals established by the Independent Commission.**

If the Congress chooses not to create such an Independent Commission, these critical issues will, nevertheless, require the urgent attention of policymakers in a system of political pressure and other factors that have, to date, proven to be incapable of satisfactory resolution.

Regardless of whether the Independent Commission is created, are several additional CIP issues require immediate attention.

Developing Threat Assessments

The lack of a comprehensive assessment of threats to U.S. infrastructures significantly hampers defensive measures and preparedness activities. DHS will eventually establish the process for vulnerability assessment and "mapping" of the nation's critical infrastructure. But that process must be informed by a clear articulation, on a continuing basis, of threats—strategically, operationally, and tactically. To the best of our knowledge, no comprehensive threat assessment exists to inform the process that DHS must manage.

Recommendation: That the President direct that the National Intelligence Council perform a comprehensive National Intelligence Estimate on the threats to the nation's critical infrastructure

Creating More Effective Cyber Security Policy

DHS will be responsible for executing operations for CIP. But it will not, apparently—and logically so—be responsible for the development of all CIP policy. We assume that CIP strategic policy development will continue to be accomplished within the White House. But the continuing bifurcation of policy for the physical and cyber components of CIP has, as we have noted above, created confusion and resulted in less than effective policy formulation.

Recommendation: That the President direct the merger of physical and cyber security policy development into a single policy entity in the White House

Enhancing Aviation Security

Securing aircraft from all potential terrorist hazards is a very difficult task. In general, these hazards can be caused by passengers (i.e., the terrorists themselves) or cargo placed on the aircraft as baggage or non-passenger cargo (e.g., mail or general cargo). Progress in meeting airline passenger baggage-screening goals has been slow, and no screening technology will ever be foolproof. Perhaps equally important is the fact that much of the non-passenger cargo on commercial passenger aircraft is not being screened.[195] This task is hindered by physical (e.g., space for screening equipment) and technical limitations (e.g., a lack of screening equipment for large, bulky cargo). Furthermore, it is expensive and time consuming.

Recommendation: That DHS elevate the priority of measures necessary for baggage and cargo screening on commercial passenger aircraft, especially non-passenger cargo

Similarly, security of general aviation aircraft and facilities is thin, where it exists at all. Cargo aircraft, in particular, pose a significant danger that is not now adequately addressed, in that they have the potential to cause even greater damage than passenger aircraft if flown into a building or other ground target, because of the added kinetic energy provided by their substantially greater weight. Cargo flown on them is frequently not adequately screened for the reasons articulated above. Furthermore, measures to secure access to them are not nearly as rigorous as for passenger aircraft. Prudent measures can be undertaken at relatively low costs, especially controls on access to aircraft and ramp and hangar facilities where aircraft are parked or stored.

Recommendation: That DHS, in conjunction with the airline industry, develop comprehensive guidelines for improving the security of general aviation

[195] Greg Schneider, "Terror Risk Cited For Cargo Carried On Passenger Jets," *Washington Post*, June 10, 2002.

Improving the Security of Dams

Hydroelectric and other dams on various watercourses present a significant hazard if terrorists find ways to exploit their controls. According to the U.S. Army Corps of Engineers National Inventory of Dams,[196] approximately 80,000 dams exist in the United States, of which approximately 24,000 would cause downstream loss of life if catastrophically breached. Of these, the Federal government owns approximately 2,100, with State and local governments and private sector organizations (e.g., utilities) owning the remainder.

The risks to dams varies, as does the ability of owners to provide adequate protection. No database currently contains the information needed to assess the risk to dams, and no national program exists for securing dams. This may stem from the fact that dams do not fall cleanly in any one infrastructure, but rather can be considered as part of the transportation, energy, and water infrastructures in different locations and circumstances. Threats to dams range from terrorist attacks to cyber intrusions. At least one recent incident has occurred of a teenage cyber "hacker" getting deep inside the control mechanisms for a series of dams in one State.

Recommendation: That DHS make dam security a priority, and consider establishing regulations for more effective security of dam facilities

Using Models and Metrics

One of the critical shortcomings in structuring programs and securing funds to protect critical infrastructures is the lack of risk-based models and metrics that help explain the value of protective measures in terms that public and private sector decisionmakers understand. Homeland security investment decisions are currently based on analysis of available information but the process for developing that information is far from rigorous. Many such investment decisions are based on partial descriptions of the problem and anecdotal evidence. However, by virtue of its enabling legislation, DHS will own the National Infrastructure Simulation and Analysis Center.[197] This asset provides DHS with a world-class modeling and simulation capability, expert analysts, and the opportunity to use these abilities and expertise to enhance CIP programs and guidelines.

Recommendation: That DHS use NISAC modeling and analytic capabilities to develop metrics for describing infrastructure security in meaningful terms, and to determine the adequacy of preparedness of various critical infrastructure components

[196] Available at www.crunch.tec.army.mil/nid/webpages/nid.cfm
[197] See http://www.sandia.gov/CIS/NISAC.htm.

CHAPTER IX. ESTABLISHING APPROPRIATE STRUCTURES, ROLES, AND MISSIONS FOR THE DEPARTMENT OF DEFENSE

A type of military motto has developed over time: "The mission of the U.S. Armed Forces is to fight and win the Nation's wars." For the past century, except for one incident, that has essentially meant fighting those wars on foreign soil. But the war on terrorism has come to our shores, and the actual as well as the perceived level of security we have historically enjoyed has been demonstrably challenged.

In light of what happened on September 11, 2001, and in the intervening months, it may now be necessary to return to some basic tenets on which the Republic was founded, and the Constitution of the United States of America is the appropriate starting point.

> *ARTICLE IV, Section 4. The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion; and on application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence.*

Understanding the Proper Role of the Military in Homeland Security

Although our military forces have been designed to fight our Nation's wars within a context of forward deployment and engagement, there is no question that some of the Department's warfighting capabilities and resources are also applicable to homeland security.

At times, using the military domestically raises difficult issues about the division of State and Federal power. Unless they occur on a Federal reservation, and sometimes even then, homeland security responses will likely begin with the local and State responders. Within a State, the governor controls the National Guard and the State emergency management agency when an incident is controlled or managed by the State. When U.S. active duty and reserve forces become involved, they serve under the President. The President also has the Constitutional power to federalize the National Guard for various contingencies.

Using the military for homeland security inevitably has raised concerns about the proper roles and rules for use of the military domestically. There are several laws that proscribe the use of active duty forces domestically, the most widely known being the Posse Comitatus Act.[198] The existence of such laws is an indication of the concern within the country that the military not be misused. As the Advisory Panel has noted in a previous report, there is a significant problem in implementation of these laws caused by the widespread confusion about their interpretation and how they apply to specific situations. As a result, military response to many homeland security situations may be delayed in order to work through the legal issues.

[198] 18 U.S. Code, Section 1385. For a complete discussion of the laws for use of the military domestically, see our *Second Report*, Appendix R, and our Third Report, Chapter VI.

The new *National Strategy for Homeland Security* acknowledges the important role of the military in homeland security.[199] In this context, "homeland security" is an overarching term comprising two missions: "homeland defense" and "civil support."[200] According to the Department of Defense (DoD), the term homeland defense refers to military combat missions; that is, military sea, air, and, land operations wherein DoD leads and other Federal agencies may provide support. Operation Noble Eagle, which provides for air defense of U.S. territory against terrorist attacks, is a recent example.

Providing for the Defense of the Homeland

That the military has a clear mission to provide "homeland defense"—one in which it "would take the lead in defending the people and the territory of our country, supported by other agencies"— is a clear and sober fact recognized by the new *National Strategy for Homeland Security*.[201]

In its *Second Report*, the members of this panel, with a single exception, made an explicit recommendation about the use of the military:

> *We recommend that the President always designate a Federal civilian agency other than the Department of Defense (DoD) as the Lead Federal Agency.*

We made that recommendation in the context of the potential involvement of multiple Federal, State, and local entities being engaged in a response to a planned or potential terrorist attack. A word of clarification about our previous recommendation is, perhaps, now in order. We recognize that certain responses to attacks may be exclusively or at least primarily military missions. The attacks of September 11 of last year are instructive. After the two hijacked airliners crashed into the Trade Center towers and a third crashed into the Pentagon, it was quickly discovered that a fourth had also been hijacked and had turned toward the Nation's Capital. We now know that, but for the courageous and heroic intervention of some of our fellow citizens, United Airlines Flight 93 may have been shot down by Air Force fighters launched to intercept it. We now acknowledge that, for certain actions by terrorists that may rise to the level of an "invasion"—from the air, from the sea, and potentially even from land external to the United States—the military may have to take the lead in responding. In certain circumstances, no other agency of government, at any level, will likely have the capability to respond to such attacks. That concept is firmly embedded in the formation of the new U.S. Northern Command, discussed in greater detail below.

Providing Military Support to Civil Authorities

The new *National Strategy* also recognizes that the Department of Defense has an additional significant homeland security mission—military support to civil authorities. This is not a totally new mission. The military regularly is called on to provide assistance to civil authorities to deal

---

[199] *The National Strategy for Homeland Security* (Washington, DC: The White House, Office of Homeland Security, July 16, 2002), p. 13, available at online at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
[200] In this report, we use interchangeably the terms "civil support" and "military support to civil authorities."
[201] *National Strategy,* p. 13.

with natural disasters (e.g., hurricanes, floods, and fires), as well as manmade incidents (e.g., riots and drug trafficking).

The military is called on to perform these missions because it moves and organizes large numbers of trained personnel to provide a coordinated response to incidents at home and because the military has developed specialized capabilities (particularly medical, engineering, and chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) weapon response capabilities) that either do not exist at the State and local level or do not exist in sufficient quantities. In using the military domestically, a number of legal and political issues arise.

Increased homeland security concerns also have focused attention on the National Guard's domestic role. Given its nationwide disposition and connection to local communities, the Guard is arguably well suited to provide assistance when civilian capabilities are overwhelmed in an emergency. However, the National Guard is also an important part of the U.S. military's power projection capability. Therefore, devoting National Guard resources to homeland security and the potentially competing demands of foreign warfighting have consequences for both that need to be considered. We discuss the role of the National Guard in greater detail below.

DoD defines civil support as mutual support activities it undertakes with any civil government agency for planning or responding to the "consequences of civil emergencies or attacks, including national security emergencies." Civil emergencies include "any natural or manmade disaster or emergency that causes or could cause substantial harm to the population or infrastructure."[202] The 2002 deployment of military forces to assist Federal border security agencies is a recent example of a civil support operation.

For those missions involving military support to civil authorities, the Advisory Panel reaffirms the normal—and logical—sequence of commitment for response to a terrorist attack outlined in its *Second Report*, and for the appropriate place for employment of military forces. In this regard, response to terror threats or attacks will be led by first responders, those who serve the communities in which the incident has occurred. Responding second are those organizations mobilized under the leadership and authority of the State governors (including the National Guard of the several States), including requests for assistance from a full range of State and Federal law enforcement agencies. Within this context, a governor could request assistance from National Guard units from adjoining States under voluntary State compacts. At the point when response requirements exceed the State's capacity, a governor could request assistance from the President, who would designate a Lead Federal Agency to manage the U.S. response. The Advisory Panel has recommended in past reports that the Lead Federal Agency be a civilian agency, rather than the Department of Defense. The President's assistance might include the deployment of Federal military forces as a last resort.

The military has a long history of providing support to civil authorities to deal with natural and manmade disasters. This assistance is now common: between 1998 and 2000, the military

[202] Department of Defense, Directive 3025.15 (Washington, DC: Department of Defense, Office of the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict, 18 February 1997), sections E2.1.3 and E2.1.9.

supported an average of 73 events per year.[203] Large-scale incidents can create significant demand for military forces. Notable examples of such incidents in the last decade, beyond the post – September 11 activities, include the Los Angeles Riots and Hurricane Andrew in 1992, the 1995 bombing of the Murrah Federal Office Building in Oklahoma City, Hurricane Floyd in 1999, the Western forest fires of 2000, and the 2002 Olympics in Salt Lake City.

Each homeland security incident that requires military support to civil authorities will involve a unique size and mix of forces. Specialized military capabilities are deployed as required and responding forces also typically include general-purpose units and military police; air transportation; engineers; signal operators with communication equipment; medical experts; and a command element with expertise in the law, public affairs, and intergovernmental coordination.

While the military participates in numerous missions to support civil authorities each year, the Department of Defense does not count this support as its primary mission. Warfighting is the Department's primary mission and takes priority unless the Secretary of Defense directs otherwise.[204] Therefore, with the exception of a limited number of specially-trained units (e.g., the National Guard's Weapons of Mass Destruction Civil Support Teams (WMDCSTs), the forces DoD provides to support civil authorities are primarily trained to perform their warfighting missions. In addition, these forces may not always be available. While demand for military civil support operations may increase in the future, so might the military's warfighting commitments increase (e.g., for the global war on terrorism or a conflict in Iraq[205]). Therefore, we must consider what homeland security capabilities we are counting on DoD to provide, whether it is the most appropriate provider of those capabilities, and how to handle simultaneous demand for overseas warfighting and homeland security missions.

The President has recognized the challenges ahead in his *National Strategy for Homeland Security*. The *National Strategy* has identified three broad roles the military might be called upon to perform domestically, including executing homeland defense missions with support from other agencies, responding to emergencies to provide capabilities that other agencies do not have, and supporting the lead Federal agencies for "limited scope" missions such as national security special events. The strategy also provides details on potential DoD combating terrorism operations: "Military support to civil authorities pursuant to a terrorist threat or attack may take the form of providing technical support and assistance to law enforcement; assisting in the

[203] LTC James Rice, United States Army, Deputy Special Assistant for Military Support, Office of the Secretary of the Army, remarks before the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, September 30, 2002, Arlington, Virginia.

[204] An analysis of the Defense Department's combating terrorism directives has determined that "the military's non-MSCA [military support to civil authorities] operations take priority, unless the Secretary of Defense determines otherwise." This guidance on civil support is provided in Department of Defense Directive 3025.1, at A.2.-6. The analysis is presented in Barry Kellman, *Managing Terrorism's Consequences: Legal Issues* (Oklahoma City: Oklahoma City National Memorial Institute for the Prevention of Terrorism, March 2002), chap. 2, p. 14.

[205] According to an official in the office of the Defense Department's Director of Military Support, a large-scale conflict abroad, with Iraq for example, could significantly reduce the military resources available at for civil support operations in the U.S. homeland. COL Ricki L. Sullivan, Chief, Military Support Division, Department of the Army, RAND staff interview, the Pentagon, Arlington, Virginia, November 7, 2002.

restoration of law and order; loaning specialized equipment; and assisting in consequence management."[206]

Reviewing the historical support that the military has provided to civil authorities can help us anticipate the kinds of support and level of effort that the military may be called upon to provide in the future to respond to terror attacks. After the Oklahoma City bombing, the U.S. military deployed about 800 active and reserve personnel, while the Oklahoma National Guard provided 465.[207] The military support provided included medical and rescue teams, structural experts, and air and ground transportation. After the September 11 attacks, DoD provided 657 active duty personnel to support response operations at the Pentagon and the World Trade Center. DoD support deployed to the Pentagon included a defense coordinating element, logistics support, and engineers. Most of the active duty military support at the World Trade Center came from the 387 personnel manning the hospital ship *Comfort*, but it also included a defense coordinating element, a medical mobilization center, logistics support (airlift), and subject matter experts on demolitions and remote sensing operations.[208] The National Guard provided the lion's share of the military forces responding to the crisis in New York City. At their peak, a total of 5,070 New York and 1,006 New Jersey National Guardsman were committed to the effort.[209]

Given its size, nationwide disposition, and inherent capabilities, the Army, including the Army National Guard, can be expected to provide most of the military support in the event of future attacks with CBRN weapons. The Army's potential level of effort for such incidents has been estimated by extrapolating from past support operations. Using this approach, RAND estimates that an Army response could range from approximately 4,000 soldiers for a small biological or radiological attack, to more than 20,000 to respond to a large-scale anthrax attack in which more than 15,000 people have been exposed.[210]

IMPROVING STRUCTURES FOR THE USE OF THE MILITARY DOMESTICALLY

New homeland security missions for combating terrorism warrant dedicated civilian and military organizational structures. Since the terrorist attacks of September 2001, the Department of Defense has restructured both the civilian oversight roles and the military organizations that deal with homeland security. In this report, we assess the progress in both organization and missions for providing military support to civil authorities, and recommend further improvements for military capabilities that may strengthen the Nation's ability to combat terrorism.

---

[206] *The National Strategy for Homeland Security*, (Washington, DC: The White House, Office of Homeland Security, 16 July 2002), available at online at http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
[207] "After Action Report for Oklahoma Bombing Incident of 19 Apr 95," completed by the Fifth U.S. Army and Fort Sam Houston, August 17, 1995.
[208] Department of the Army, Office of the Director of Military Support, information paper, "DOD Support to the Events of and Subsequent to Sept 11th 2001," Undated.
[209] Office of the Director of Military Support, information paper, "DOD Support."
[210] Richard Brennan, "U.S. Army Finds Its Role at Home Up for Grabs," *Rand Review,* Vol. 26, No. 2, Summer 2002 (Santa Monica: RAND, 2002), p. 47; and Eric V. Larson and John E. Peters, *Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options* (Santa Monica: RAND, 2001), p. 167.

Organizing the Defense Civilian Structure for Homeland Security

Decisions to deploy military forces for homeland security activities are not made by the uniformed military; such decisions are made by the Secretary of Defense, or his designated agent. The Department of Defense is reorganizing both the military command structure and the civilian oversight structure dedicated to homeland security. In November 2002, Congress approved the request from the Secretary of Defense to create a new Assistant Secretary position within the Office of the Secretary of Defense to oversee the support that the military provides for homeland security. We congratulate the Congress and the Administration for creating this new position. This office will formulate DoD homeland security policy and oversee the approval of military contributions to the national homeland security effort. In situations where the lead Federal agency (most likely either the Department of Homeland Security or the Department of Justice) determines it needs military assistance, it would direct a request to the Secretary of Defense. To expedite the process, decisional authority is anticipated to be delegated to the new Assistant Secretary for Homeland Defense; however, the Secretary of Defense will retain approval authority for responses to acts of terrorism, deployment of assets to deal with CBRNE, and military assistance for civil disturbances. The Assistant Secretary of Defense would review the request and, if it were determined that DoD can meet the request, would direct the Joint Staff to select the military assets that will be used and issue deployment orders.

In this arrangement, the Assistant Secretary of Defense for Homeland Defense will assume the role that the Secretary of the Army (i.e., as the Secretary of Defense's Executive Agent for civil support) and his Director of Military Support (DOMS) filled in the past. The ASD Homeland Defense will have a much broader portfolio than DOMS had, because he will be responsible for all DoD homeland security support to Federal, State, and local authorities as well. In most cases DoD would play a supporting role in homeland security; however, there are some cases when the President might order the military to take the lead to thwart a terrorist attack. Oversight of preparations for such activities to combat terrorism is vested by the Secretary of Defense in the Under Secretary for Policy and the Assistant Secretary for Special Operations-Low Intensity Conflict (SOLIC).

We have noted here important developments in DoD's organization. The panel reaffirms its view that command and control relationships must be very clear and practiced. Responsibilities and authorities must be clearly prescribed and exercised. However, it is also important for DoD to articulate the many changes it is making so that the American people understand how their government is moving to protect them from new threats. As such, the Advisory Panel applauds Congress for directing the Secretary of Defense to submit a detailed report describing DoD's homeland security responsibilities and how it is preparing to discharge them.[211]

Organizing the Military Structure for Homeland Security

In our *Third Report*, we recommended "that the National Command Authority establish a single, unified command and control structure to execute all functions for providing military support or assistance to civil authorities." A new geographic combatant command, U.S. Northern Command (NORTHCOM), has been established in the Unified Command Plan, effective October 1, 2002.

[211] U.S. House, 107th Congress, 2nd Session, Conference Report on H.R. 4546, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*, November 12, 2002, section 1404.

Based at Petersen Air Force Base in Colorado, the new command has been assigned the mission of defending the continental United States, Alaska, Puerto Rico, and the U.S. Virgin Islands and for providing military support to civil authorities.[212] The Command describes its mission, inclusive of both its homeland defense and civil support responsibilities, as follows:

> *The command's mission is homeland defense and civil support, specifically:*
>
> - *Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within the assigned area of responsibility; and*
> - *As directed by the President or Secretary of Defense, provide military assistance to civil authorities including consequence management operations.*[213]

NORTHCOM is in a transition between initial operational capability and full operational capability. In its initial structure, NORTHCOM has few permanently assigned forces, and most of them serve as part of its homeland security command structure. NORTHCOM's commander will exercise combatant command authority over his own headquarters in Colorado Springs, the Joint Force Headquarters Homeland Security (JFHQ- HLS), the Joint Task Force 6 (JTF-6) counterdrug headquarters, and the Joint Task Force Civil Support (JTF-CS), which provides command and control for all Federal military forces operating in support of a lead Federal Agency to manage the consequences of CBRNE incidents. Commander NORTHCOM may also exercise combatant command authority over the Cheyenne Mountain Operations Center.

The JFHQ-HLS, located in Norfolk, Virginia, was established by Joint Forces Command immediately after September 11, 2001 to coordinate the land and maritime defense of the continental U.S. as well as military assistance to civil authorities for "all hazards." At NORTHCOM's initial operational capability, combatant command over JFHQ-HLS was transferred to NORTHCOM. The ultimate role and status of this headquarters is pending design determination of NORTHCOM at full operational capability. The Commander of NORTHCOM also serves as Commander, U.S. Element NORAD, and currently as commander of NORAD, the U.S.-Canadian Aerospace Defense Command. In these, roles he conducts and coordinates North American air defense. NORTHCOM, at least initially, does not have control of any other units. As is the case with other regional combatant commanders, Joint Forces Command (JFCOM) will act as NORTHCOM's primary "force provider" if additional units or personnel are needed for any planned or contingency operations and for exercises. As such, NORTHCOM will only be given control of air, land, sea, and maritime forces when required to perform an assigned task.

Although NORTHCOM's mission statement implies that the Command could be directed to execute *counterterrorism* operations in support of civil authorities,[214] we are not aware of any deliberate planning by the Command to support such a contingency. Conceivable events (e.g., multiple, geographically dispersed terrorist operations within U.S. territory) might exhaust civil

---

[212] U.S. Pacific Command has responsibility for Hawaii.

[213] NORTHCOM Mission Statement, available at http://www.northcom.mil/index.cfm?fuseaction=s.whoweare&section=3, accessed on December 5, 2002.

[214] DoD defines counterterrorism as "offensive measures taken to prevent, deter, and respond to terrorism." It defines antiterrorism as, "Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military forces." See Department of Defense, *DoD Dictionary of Military and Associated Terms*, Joint Publication 1-02, as amended through August 14, 2002, available at on the internet at http://www.dtic.mil/doctrine/jel/doddict/index.html.

and other limited military resources envisioned for use in existing national plans. Moreover, scenarios exists within which NORTHCOM might then be directed to provide additional support to civil authorities *regardless* of its pre-incident focus on planning and training for the so-called "consequence management" mission. We have consistently noted in this and earlier reports that ample statutory authority already exists for use of the military to provide a wide range of support to civil authorities, including very specific types of support under special terrorism statutes,[215] as well as more general authority under such other provisions as the Insurrection Statutes.[216]

Recommendation: That the Secretary of Defense clarify the NORTHCOM mission to ensure that the Command is developing plans across the full spectrum of potential activities to provide military support to civil authorities, including circumstances when other national assets are fully engaged or otherwise unable to respond, or the mission requires additional or different military support. NORTHCOM should plan and train for such missions accordingly

The creation of NORTHCOM is an important step toward enhanced civil-military integration for homeland security planning and operations and could result in an enhancement of homeland security response capabilities. NORTHCOM has the responsibility to plan for a number of critical military homeland security activities. NORTHCOM will need to train and exercise with civil authorities at all levels of government—Federal, State, and local. Given its command relationships, Commander NORTHCOM will be well positioned to ensure unity of command and effort when military units are employed for homeland missions under Federal authority.

In our *Third Report*, we recommended that a unified command be created "to execute all functions for providing military support or assistance to civil authorities"—an all-hazards approach. The Advisory Panel is pleased that NORTHCOM will apparently execute *most* of these functions, and adds the following:

Recommendation: That the NORTHCOM combatant commander have, at a minimum, operational control of all Federal military forces engaged in missions within the command's area of responsibility for support to civil authorities

IMPROVING MILITARY CAPABILITIES FOR HOMELAND SECURITY

The Administration and Congress have improved the Federal government's structure for the delivery of military support to civil authorities. However, the panel believes additional enhancements are possible and necessary. The President and Congress should clarify legal authorities for military activities within U.S. territory. Training for civil support operations should be increased across the armed forces. As the panel notes in Chapter V, Organizing the National Effort, and later in this chapter, the President and the Congress should initiate a rigorous assessment of national preparedness requirements. That assessment should be used to evaluate further enhancements to the military's ability to deliver needed capabilities as part of the national homeland security effort. Finally, the National Guard's homeland roles and missions must be reevaluated in light of the new security environment facing the Nation.

[215] 10 U.S. Code, Section 1282, and 18 U.S. Code, Section 831.
[216] 10 U.S. Code, Sections 331 et seq.

Clarifying Posse Comitatus and Other Relevant Statutes

Currently, there is a debate within the country on the authorities granted by the Posse Comitatus Act. Historically, Americans have been hesitant to use the armed forces for internal security. In general, the Posse Comitatus Act prohibits the Federal military's participation in front-line law enforcement activities, such as arrest, search, seizure, surveillance, or pursuit of convicted or suspected criminals. Some believe the laws governing the domestic use of the military should be modified to tighten restrictions on military law enforcement activities. But in the last year, the military has been used in new ways to support homeland security missions. For example, in October 2002 military reconnaissance aircraft were used in an attempt to locate the sniper terrorizing the Washington, DC area. Some leading members of Congress believe the time has come to re-examine the 1878 law in light of the new security environment the Nation faces.[217] In considering the role of the military in homeland security and its use in support of civil authorities, the Advisory Panel reviewed again the authorities granted in current law to assess its position on the debate.

The President's homeland security strategy calls for a "thorough review of the laws permitting the military to act within the United States in order to determine whether domestic preparedness and response efforts would benefit from greater involvement of military personnel and, if so, how." The panel previously noted that significant statutory and regulatory authority already exists for using the military inside the United States, especially under the insurrection statute.[218] However, there remains widespread confusion about Posse Comitatus and other statutes that address domestic use of the military. For that reason, the Advisory Panel supports the review proposed by the Administration in the *National Strategy* as a means to bring clarity to this important issue.

To achieve that clarity, the laws governing domestic use of the military should be consolidated and the Federal government should publish a document that clearly explains these laws.[219] In consolidating the laws, the legislation should clarify ambiguities about the authority to use the military to respond to terrorist acts involving chemical, biological, radiological and/or nuclear weapons as well as conventional or cyber attacks.

Recommendations: That the President and the Congress amend existing statutes to ensure that sufficient authorities and safeguards exist for use of the military across the entire spectrum of potential terrorist attacks (including conventional, chemical, biological, radiological, and nuclear threats as well as cyber); that the authorities be consolidated in a single chapter of Title 10; and that DoD prepare a legal "handbook" to ensure that military and civilian authorities better understand the

---

[217] These positions are detailed in Pat Towell, "Northern Command Stirs Issue of Military's Role in Security," *Congressional Quarterly Weekly*, 2 November 2002, p. 2867; and Harry Levins, "Loopholes in Law Give Military Ability to Play Role in U.S.," *St. Louis Post-Dispatch*, 21 April 2002.

[218] See *Second Annual Report*, page 27 and Appendix R. http://www.rand.org/nsrd/terrpanel/

[219] In April 2001 the Department of the Army's Center for Law and Military Operations published an "advisory" guide entitled *Domestic Operational Law Handbook for Judge Advocates*. Although its contents do not represent official DoD legal positions, the Army guide could serve as the basis for an official DoD handbook of the type we recommend. The Army's guide is available at on the internet at https://www.jagcnet.army.mil/clamo/publications.

legal authorities governing the use of the military domestically in support of civilian authorities for all hazards—natural and manmade

Identifying Requirements

Northern Command and supporting service and Joint Staff structures have the capability to identify purely military homeland defense requirements for land, maritime, and air combat missions. The problem, however, is that no process is clearly in place to identify among the full scope of participants the requirements for support to civil authorities. It is critical that States, cities, and municipalities define requirements beyond their current capabilities that should be met by Federal augmentation.

Recommendation: That the President direct the DHS to coordinate a comprehensive effort among DoD (including NORTHCOM) and Federal, State, and local authorities to identify the types and levels of Federal support, including military support, that may be required to assist civil authorities in homeland security efforts and to articulate those requirements in the National Incident Response Plan

The DHS should evaluate shortfalls and allocate augmentation responsibilities to other Federal agencies, including DoD. DHS should articulate those responsibilities in the National Incident Response Plan. The Defense Department, supported by NORTHCOM, should give DHS full cooperation in completing this effort.

Enhancing Training

Military personnel in the United States have long adhered to this principle: "train as you fight and fight as you train." This principle is certainly valid for homeland defense and civil support operations. The panel is reasonably confident that NORTHCOM will develop adequate plans for its homeland defense, military-led mission and that most combat training and exercises for military units will have some application in that mission. Nevertheless, there will be special considerations for conducting military operations inside or over the United States and in adjacent waters—proximity to the civilian population, coordination with other governmental entities, and air or sea traffic issues, as examples—that will need significant attention in training and exercises. Moreover, States and localities should be provided information and definitive guidance on what to expect in the event of future homeland defense, military-led operations.

In addition, the panel is concerned that there is no assurance that specially trained forces will be available to NORTHCOM prior to a crisis, and that current civil support training across the armed forces in general is insufficient.

Although the military trains extensively for combat operations, training for homeland activities differs in essential ways. Compared to coordination within a purely military command structure, coordinating homeland operations with other Federal, State, and local authorities will require comparable skills but different applications. Liaison activities among the elements involved in planning, training, and exercising will take on greater importance. For response operations, command and control processes may be different. Requirements for joint training will take on a new meaning, as joint exercises with State and local responders will be very important. Finally, certain homeland missions will require support to civil law enforcement and the execution of law

enforcement tasks. Military personnel will require specific training to support local law enforcement agencies in performing law enforcement missions.

The *problem* has been that insufficient attention has been paid to and resources made available for civil support training. We now know the pervasiveness of the threat, the increased probabilities of terrorist acts, and the need for enhanced preparation for effective response. Therefore, the Advisory Panel suggests a significant increase in the emphasis on civil support missions for all hazards incidents, with special emphasis on response to acts of terror. Specifically, the Department of Defense should increase the planning, training, and exercising of Active, Guard, and Reserve forces to execute civil support missions.

Recommendation: That the Secretary of Defense direct that all military personnel and units under NORTHCOM, or designated for NORTHCOM use in any contingency, receive special training for domestic missions. Furthermore, in those cases where military personnel support civil law enforcement, special training programs should be established and executed.

Establishing New Capabilities for Military Support to Civil Authorities

As noted above, NORTHCOM's initial force structure will include few permanently assigned forces.[220] The problem with this initial force structure is that it leaves unanswered questions about the scope and level of training and exercising of units and personnel that might be used for civil support missions. It is not clear that Commander NORTHCOM's pre-incident authorities have been aligned with the civil support responsibilities that he has been assigned. Indeed, there are no assurances that civil support training will be conducted unless NORTHCOM is given command of specific units, some other pre-incident authority over units, or specific units commanded by others are designated and trained for civil support missions.

[220] The panel acknowledges that NORTHCOM is not unique with respect to the provision of assigned forces but argues nonetheless that NORTHCOM is unique among commands. For example, like NORTHCOM, U.S. Central Command (CENTCOM), the Unified Command in charge of military operations in an area including the Middle East, Central and Southwest Asia, and Northeast Africa, does not have permanently assigned forces. However, CENTCOM can be assured that forces temporarily assigned will be fully ready for combat missions that might occur in its area of responsibility. This is because military units have been notified that they are part of a CENTCOM operational plan and must train for that mission. NORTHCOM, on the other hand, if it is assigned forces temporarily when an incident occurs, cannot be assured that those forces will have been trained specifically for homeland security missions, especially civil support missions, because no formal contingency plans currently exist that would trigger a requirement for training. Forces provided to NORTHCOM will most likely be trained for warfighting not necessarily for homeland defense or for civil support missions.

Our understanding of the latest plan for NORTHCOM command authorities is that its commander will have a "combatant command"(COCOM)[221] relationship with the various service component commands (i.e., ARNORTH, NAVNORTH, NORTHAF, MARFOR NORTH). Its full implications are not yet clear. There is a question about this whether command relationship is only for the purpose of unity of *homeland defense* authority and responsibility or applies more broadly to all *homeland security* missions, including NORTHCOM's civil support mission. Thus, at this writing, the extent to which the new command will be able to direct new and expanded civil support training and exercises remains unclear.

Recommendation: That the Secretary of Defense clarify NORTHCOM's combatant command authority to ensure that Commander NORTHCOM can direct subordinate commands to conduct pre-incident planning, training, and exercising of forces required to conduct civil support missions

The Advisory Panel acknowledges that the U.S. military is rightly focused on warfighting. However, the panel believes many of its concerns related to pre-incident planning, training, and exercises could be rectified if NORTHCOM were assigned forces for civil support missions. Indeed, the possibility of a major attack on U.S. soil of a size that would overwhelm even the best-prepared cities and States warrants consideration of dedicating a small number of specialized, "rapid reaction" forces to NORTHCOM for civil support. The advantages of dedicated forces are that they can respond quickly and can be well trained to operate effectively at the scene.

Currently, DoD has several small, specialized units that are prepared to quickly deploy to support civil authorities in dealing with a terrorist attack. (Appendix P lists units and assets identified by the Office of the Secretary of Defense as having a homeland CBRNE response or other civil support mission.) The Department has, for example, units that, under certain circumstances, could respond to ongoing terrorist or hostage situations that exceed the capability of law enforcement agencies. The employment of these units within the United States is reserved for only the most severe circumstances. The National Guard has a dedicated but limited CBRNE response capability for homeland operations: the Weapons of Mass Destruction Civil Support

[221] As of August 2002, the Department of Defense had defined combatant command (command authority) as follows: "Nontransferable command authority established by title 10 ("Armed Forces"), United States Code, section 164, exercised only by commanders of unified or specified combatant commands unless otherwise directed by the President or the Secretary of Defense. Combatant command (command authority) cannot be delegated and is the authority of a combatant commander to perform those functions of command over assigned forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction over all aspects of military operations, joint training, and logistics necessary to accomplish the missions assigned to the command. Combatant command (command authority) should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and Service and/or functional component commanders. Combatant command (command authority) provides full authority to organize and employ commands and forces as the combatant commander considers necessary to accomplish assigned missions. Operational control is inherent in combatant command (command authority). Also called COCOM." *DoD Dictionary of Military and Associated Terms*, Joint Publication 1-02, as amended through 14 August 2002, available at on the internet at http://www.dtic.mil/doctrine/jel/doddict/index.html

Teams.[222] Several small active duty response teams have been specially designed to deal with CBRNE events. However, other than the WMDCSTs, those additional existing CBRNE response teams are deployable to theaters abroad.[223] In addition, existing CBRNE response teams, including the WMDCSTs, are designed to provide a command capability, or specialized capability (e.g., chemical or biological agent decontamination), or technical advice and a communications channel to follow-on forces. They could not by themselves handle medium- or large-size events.

The Army has brigade-size elements (e.g., comprising roughly 3,500 airborne troops[224]) standing by for rapid deployment to trouble spots throughout the world. Similar capabilities for rapid deployment exist in the Air Force, Navy, and Marine Corps. Analogous rapid response-type capabilities should arguably be tailored to deal with homeland terrorist events that overwhelm State and local capabilities. Although the Advisory Panel fully understands the principle of forward defense, we believe military organizations should be established, trained, and dedicated to homeland defense *and* civil support missions if the *National Security Strategy of the United States of America* is to be meaningful—that "our military's highest priority is to defend the United States." Our belief is premised upon the fact that the territory of the United States is now a battlefield in the war on terrorism.

Recommendation: That the Combatant Commander, NORTHCOM, have dedicated, rapid-reaction units with a wide range of response capabilities such as an ability to support implementation of a quarantine, support crowd control activities, provide CBRNE detection and decontamination, provide emergency medical response, perform engineering, and provide communication support to and among the leadership of civil authorities in the event of a terrorist attack

---

[222] In the Fiscal Year 2003 Defense Authorization Act, Congress directed the Secretary of Defense to establish WMDCSTs in each of the remaining States and territories; thus, a total of 55 teams have been authorized, with two stationed in California. Each team has 22 personnel. U.S. House, 107th Congress, 2nd Session, Conference Report on H.R. 4546, *Bob Stump National Defense Authorization Act for Fiscal Year 2003*, November 12, 2002, section 1403.

[223] According to an official in the Office of the Assistant Secretary of Defense for Reserve Affairs (OASD-RA), the WMDCSTs are dedicated to homeland operations in accordance with the Unified Command Plan. In Appendix P, numerous other military units and assets are also described. Most of these have varying levels of commitment to homeland operations and, depending on the level of effort demanded by concurrent incidents, at least some likely could perform missions at home and abroad simultaneously. According to OASD-RA, the Marine Corps' Chemical Biological Incident Response Force, although deployable abroad, is in fact focused on homeland operations. The CBIRF maintains 90 Marines in a 24-hour readiness posture for immediate response and a follow-on force of 200 more personnel. In addition, OASD-RA says the Army's Technical Escort Unit and 52nd Ordnance Group are deployable but maintain elements dedicated to supporting U.S. civil agencies (e.g., the FBI). Finally, in the event of a terrorist incident, commanders of military installations within U.S. territory are authorized to provide "immediate response" to requests from civil authorities "to save lives, prevent human suffering, or mitigate great property damage." Therefore, communities in proximity to U.S. military installations could in most circumstances expect resident military personnel and civilian employees to render general assistance in a crisis; such assistance would be reasonably assured if pre-preplanned in the form of a civil-military mutual aid agreement. On installation commanders' immediate response authorities, see Kellman, *Managing Terrorism's Consequences,* chapter 2, p. 13.

[224] Army light infantry, airborne, and air assault brigades typically have between approximately 3,200 and 3,500 soldiers. For details, see Federation of American Scientists, Military Analysis Network, "U.S. Army Table of Organization and Equipment," available at: http://www.fas.org/man/dod-101/army/unit/toe/index.html.

If NORTHCOM's Combatant Commander establishes the requirement, force "designers" and force providers should consider, in coordination with the States and local organizations, a mix of existing or specifically tailored rapid-reaction forces to meet civil support missions. Once designated, these rapid reaction forces should be under NORTHCOM's operational command. They could include forces (Active, National Guard, and Reserve) representing a full range of joint capabilities, such as military police, command and control, medical, engineering, CBRNE detection/decontamination, and liaison elements.

Improving the National Guard's Role

The National Guard's future role in homeland security activities has moved to the forefront of the debate on military support options. The Guard's history of service within the United States extends to its founding as a colonial militia during the Revolutionary War era. More recently its role in supporting the active force increased continuously during the Cold War and today is manifested in increasing numbers of deployments throughout the world, including long-term commitments in Bosnia and Kosovo.

In preparing to confront terrorists, the United States and its individual States must resolve difficult issues about the role of the States and the Federal government in protecting citizens. The National Guard's potential contribution to combating terrorism is an important dimension of the assessment of appropriate State and Federal roles because the National Guard is "dual missioned": it can serve directly both the State governor and the citizens of the State, as well as the President.

The National Guard Can Operate Under Three Authorities

In the event of a natural or manmade disaster, demand for National Guard support can escalate along a continuum that begins with a governor's call up of Guard personnel in *state active duty* (SAD) status and moves through a call to Federal service. Guard personnel in SAD status are controlled by their governor, typically compensated by their State, and perform their tasks—including assistance to law enforcement—in accordance with State statutes. If a governor believes the Guard is performing missions in support of Federal agencies, he can request moving Guard personnel to U. S. Code Title 32 status, which provides for continued State control but with Federal funding for the mission. National Guard forces in Title 32 duty status can, in accordance with State statutes, support civil law enforcement in operations to deter terrorist activities and prevent attacks.[225] The National Guard can operate in a third status when the President decides it is necessary to assume control of military support activities and activates the Guard in any State for Federal active duty under USC Title 10. Such a move extends to Guard personnel Federal pay and benefits, permits Title 10 officers to command mobilized National Guard forces, and permits the President to order federalized guard units to move between States (or out of the country) as part of any national response effort.

Each of these legal authorities has strengths and weaknesses in relation to homeland security operations. States may have difficulty funding homeland security training and operations of the

[225] As we note in our *Third Report*, "statutes and regulation in certain states . . . prohibit the use of the Guard for law enforcement activities." States can restrict the law enforcement activities of National Guard forces operating in state active duty or Title 32 status. See *Third Report*, p. 52.

Guard in SAD status, especially if their missions are conducted for extended periods. Commanders are not clearly authorized under Title 32 to expend Federal funds for training for civil support tasks.[226] Guard personnel deployed in Title 32 status for national missions (e.g., to assist in border security operations) may therefore have varying levels of training and proficiency in their assigned tasks. Under Title 32, moreover, individual States can establish procedures and rules of engagement for Guard missions, potentially resulting in no comprehensive standards covering the activities of Guard personnel supporting a national mission. Military officers in Title 32 status cannot command Title 10 forces, which limits their ability to direct available Federal resources. Title 10 forces are limited by the Posse Comitatus Act, which restricts their activities and can thus limit their ability to perform critical homeland security tasks.

Recommendation: That the Congress expressly authorize the Secretary of Defense to provide funds to the governor of a State when such funds are requested for civil support planning, training, exercising and operations by National Guard personnel acting in Title 32 duty status and that the Secretary of Defense collaborate with State governors to develop agreed lists of National Guard civil support activities for which the Defense Department will provide funds

As the United States grapples with the role of the National Guard in homeland security missions, a fundamental issue that must be addressed is the degree to which past practices and informal and formal relationships (such as State emergency assistance compacts) will be effective in an environment in which our Nation, our cities, and our communities will potentially become the battlefield. Can effective response to the war on terrorism and major CBRNE incidents within our borders be met within the current structure, practices, and command and control arrangements? What is the appropriate balance between the responsibilities of State governors and Federal authorities? What is the most appropriate and acceptable concept to support unity of effort in local, State, and Federal response to such incidents as well as extremely grave national disasters? And, what is the appropriate relationship between NORTHCOM and the National Guard?

The National Guard's experience in responding to the September 2001 terrorist attacks illustrates some of the challenges associated with its dual State-Federal mission. The magnitude of the attacks compelled an immediate national response. New border and airport security measures were required. The President wanted a coordinated national effort; the National Guard offered organized military forces that could perform these missions.

---

[226] Several National Guard officers interviewed by the panel's staff expressed the opinion that Title 32 was developed primarily for Guardsmen to train for warfighting missions and that Title 32 does not clearly authorize National Guard military support to civil authorities. The Adjutant General of Washington State, Maj. Gen. Timothy Lowenberg, expressed the view that this lack of clarity acts as a deterrent to commanders who wish to train their Guardsmen for civil support operations. Commanders might face criminal penalties under the 1906 Anti-Deficiency Act (31 USC, Section 1341) if they expend on civil support training funds appropriated by Congress to support training for warfighting missions. Indeed, the Congress had to expressly authorize the Guard's conduct of counterdrug missions while in Title 32 duty status to assure commanders that such missions would not risk a violation of the Anti-Deficiency Act. To review the legislation on National Guard counterdrug activities, see U.S. House of Representatives, Committee on Armed Services, 104th Congress, 2nd Session, *National Defense Authorization Act for Fiscal Year 1996,* House Conference Report, H. Rpt. 104-450, available at ftp://ftp.loc.gov/pub/thomas/cp104/hr450.txt.

For airport security augmentation, the President requested that governors stand up the Guard in the several States to perform the mission. The President could have mobilized the Guard for this national mission under his Title 10 authorities. Instead, he called them to duty under Title 32. Maintaining the Guard in this status allowed State units to deploy to airports within roughly one week of the order. States maintained control of their Guard resources and had greater flexibility to meet airport and other security requirements. The governors also had greater flexibility to rotate Guard personnel in and out of duty status to deal with family, business, or employment issues. Governors and Guard commanders had greater flexibility in tailoring missions, drawing from multiple units within a State rather than having total units activated under Title 10, thus placing all personnel in such units on full time duty status. Importantly, the 9,100 National Guard personnel manning airports performed their duties in accordance with State laws, policies, and rules of engagement. This led to significant variation in the Guards' activities in airports across the Nation.[227] Indeed, the varied approach among the States suggests that other processes may be required and surely would be more effective.

Deploying the Guard for border security operations posed different challenges. In this case, President Bush approved 1,600 National Guard for duty in Title 10 status. The governors initially opposed the President's decision to federalize the Guard,[228] but it was decided that the border security operation was a Federal not a State mission and the Guard had no law enforcement duties to perform. Even so, the Posse Comitatus Act undermined the Guard's utility as a Title 10 force in this mission. The Defense Department determined that Guard personnel carrying weapons within U.S. territory could only use them in self defense.[229] Most personnel went unarmed and carried out their tasks under the protection of armed Customs and INS agents. Finally, in a complex intergovernmental and Federal interagency policy and decisionmaking process involving the States, the Defense Department, INS, Customs, and the Border Patrol, it took approximately six months to complete deployment of Title 10 Guard personnel for border security.[230]

The examples cited with the Federal, State, and city response to the September 11 terrorist operations in New York and at the Pentagon suggest the challenges all entities had in responding effectively to both the incidents as well as the pending threats. Since then, we have all learned of the pervasive and growing threat we face and, as the President states, the long-term nature of the war on terrorism. The *problem* we face is to determine the optimum way to employ all assets to protect the people of the United States and to respond effectively, efficiently, and decisively for consequence management in those cases when deterrence fails. Should the United States establish more formal association among the States so that the National Guard, and other committed assets, can be optimally trained, exercised, and sustained to meet future disasters in a national effort, covering multi-State regions, but where National Guard assets remain under the control of State governors? As noted earlier, Guard units and personnel deployed in Title 32 status under the control of State governors offer great advantage to the Nation and to the Guard and its individual personnel.

---

[227] George Cahlink, "Identity Crisis: The National Guard Is Torn Between Two Missions," *Government Executive*, September 2002.
[228] The governors' concerns are cited in, Adjutants General Association of the United States, Letter to the Governors and Legislators of the Several States, Territories and the District of Columbia and to the Congress and the President of the United States, February 25, 2002, p. 4.
[229] Cahlink, "Identity Crisis."
[230] Cahlink, "Identity Crisis."

We believe that an enhanced Federal-State partnership is required to support the National Guard operating in the homeland and assisting civil authorities. Experience indicates that State and Federal leaders must have options for Federal-State arrangements beyond those currently permitted in Title 32 and Title 10. Any new arrangement should permit federally-funded, multi-State activities by Title 32 Guard personnel operating under the control of State governors and with agreed Federal-State coordination mechanisms. In developing an enhanced partnership, a key objective must be to ensure that National Guard units can effectively respond to incidents of *national* significance and do so under *State* control, thus reducing the likelihood that such units will be federalized under Title 10, with all the associated disruptions and complexities such an action entails.

Key Objective = Maximum Flexibility

Develop ways to be able to utilize the National Guard to execute "national" missions requested by the President, but operating under a Governor's control, funded with Federal funds, with an "opt out" at the State's discretion. Then train and exercise National Guard units to the same standard so they can be utilized anywhere and with units from other States.

A Federal-State arrangement meeting these general requirements could be developed based on new Title 32 authorities and by building on the concept of existing multi-State assistance compacts that employ Guard resources. In this regard, the President should establish with the governors of the several States a process by which the States will deploy National Guard forces in Title 32 status to support national missions. This arrangement should include mechanisms for collaborative mission planning and execution in accordance with agreed-on standards. Such an arrangement will ensure an efficient deployment process and increased uniformity of operations by Title 32 Guard personnel.

Many States have participated in a long-standing mutual aid agreement: the Interstate Civil Defense and Disaster Compact.[231] In addition, forty-eight States and two territories have joined a congressionally-approved Emergency Management Assistance Compact (EMAC)[232] and other arrangements that permit them to provide State National Guard assets to neighboring States to deal with an emergency. However, existing compacts typically have certain limitations, which are important in the homeland security context. These compacts are designed primarily for responding to more localized events (e.g., natural disasters), as opposed to national, all-hazards incidents. States are responsible for providing funds to train their National Guard in civil support tasks. The compacts can require the State requesting assistance to fund any National Guard response effort and they do not uniformly ensure that units from outside States will have specialized or equivalent training. Finally, Guard units deployed outside their States under the

[231] For more information on interstate assistance agreements, see our *Third Report*, Appendix I.
[232] The EMAC is codified in Federal law. Participating States and territories duplicate the Federal law in their own implementing legislation. To review the public law, see U.S. House, 104th Congress, 2nd Session, Public Law 104-321, *Granting the Consent of Congress to the Emergency Management Assistance Compact,* available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ321.104.pdf.

terms of the EMAC are not permitted to engage in law enforcement tasks[233] and require additional State or Federal authorization to use military force for any activity that is prohibited by the Federal Posse Comitatus Act (details on the legal restrictions cited here are provided in this footnote).[234]

Given the long-term threat environment, the States' existing National Guard military support arrangements must be enhanced to provide for more effective response capabilities in Title 32 duty status. A new construct must also include an improved Federal-State interface for military operations. To achieve these objectives a *regionally* organized system for providing National Guard military assistance to civil authorities should be developed. Such a system could be aligned with the 10 FEMA regions. If this were done, all assets within such regions could train, exercise, and coordinate response activities under the regional system's auspices, more broadly under NORTHCOM's leadership, or under both. A memorandum of understanding (MOU) providing key details on an improved National Guard response system could be developed by Federal and State participants. Through the MOU (or some other instrument) the governors in each region could, for instance, delegate operational control of their Guard forces—or any other agreed level of control—to a regional Guard commander, or the Adjutant General of the affected State, for crisis response activities.[235]

A regionally organized National Guard response system would, like most existing emergency assistance compacts, be voluntary. The arrangement would be a "coalition of the willing": the system's founding MOU could stipulate that any governor may forgo participation in an individual response operation.

The States would have numerous incentives to participate in a regionally organized system for National Guard military support. Increased Federal funding could be committed for a previously agreed-on list of civil support missions and for regionally-organized training and exercises. The efficient and effective delivery of Guard resources during an emergency could enable States to manage even large-scale incidents while maintaining control of their Guard personnel. Finally, to bring specialized or additional military resources to bear, coordination arrangements could be established between DoD and the leadership of the National Guard's regional response system. These arrangements would also establish mechanisms for coordinated Federal-State-local

[233] This is the opinion of John G. Hathaway, Acting Deputy Assistant Secretary of Defense for Military Assistance to Civil Authorities. John G. Hathaway, email communication to Panelist William Reno, November 18, 2002.

[234] In accordance with the EMAC legislation, National Guard units may use military force outside their State if they have "express statutory authorization" (e.g., during any incident in which the governor of the State requesting aid has declared martial law or one in which the President exercises his authorities under the insurrection statutes). In the Public Law providing congressional consent to the EMAC arrangement, the restrictive article reads as follows: ''Nothing in this compact shall authorize or permit the use of military force by the National Guard of a state at any place outside that state in any emergency for which the President is authorized by law to call into federal service the militia, or for any purpose for which the use of the Army or the Air Force would in the absence of express statutory authorization be prohibited under §1385 of Title 18 of the United States Code.'' See U.S. House, 104th Congress, 2nd Session, Public Law 104-321, Article XIII.

[235] A Federal-State arrangement exhibiting many of the characteristics recommended here has already been established for bringing military resources to bear for fire-fighting. Under this arrangement, 13 States have signed an MOU with the Secretary of the Air Force to provide for a mixed force of Title 10 and Title 32 assets in support of State fire-fighting operations. Brig Gen John E. Iffland, Commander, 146th Airlift Wing, Air National Guard, presentation to a panel member and staff, 14 November 2002, at the RAND Corporation, Arlington, Virginia.

planning, training, exercises, and operations activities by participating organizations, including such other Federal entities as the Federal Emergency Management Agency.

Recommendations: That the President and governors of the several States establish a collaborative process for deploying National Guard forces in Title 32 duty status to support missions of national significance at the President's request

That the Congress provide new authority under Title 32 to employ the National Guard (in non-Title 10 status) on a multi-State basis, and with governors' consent to conduct homeland security missions, and that the Secretary of Defense define clearly the appropriate command relationships between DoD and the National Guard

That Congress and DoD promote and support the development of a system for National Guard civil support activities that can deploy forces regionally--in coordination with DoD--to respond to incidents that overwhelm the resources of an individual State

In our *Third Report*, we recommended the following:

> "--That the Secretary of Defense direct specific mission areas for the use of the National Guard for providing support to civil authorities for combating terrorism. Further, we recommend that the Secretary:
>
> "-- In coordination with State governors, assess National Guard force structure, define appropriate roles and missions, and establish units with specific capabilities for homeland security missions.
>
> "-- Increase the percentage of full-time personnel in Guard units designated for homeland security missions and ensure that pay and benefits parallel those of active-duty service members.
>
> "-- Direct which National Guard units will be assigned homeland security missions as their primary missions with combat missions outside the United States as secondary missions and provide resources consistent with the designated priority of their homeland missions.
>
> "-- Direct that National Guard units with priority homeland security missions plan, train, and exercise with State and local agencies."

To the extent that we have not done so explicitly in this chapter, we reaffirm those recommendations but with one exception. We believe that, given the lessons learned during and after September 2001 and considering all the current circumstances and requirements, further enhancement of the National Guard's civil support capability and responsibility is necessary. We therefore expand our recommendation on roles and missions of the National Guard contained in the third "bullet" above as follows:

Recommendation: That the Secretary of Defense direct that certain National Guard units be trained for and assigned homeland security missions as their *exclusive* missions (rather than primary missions as stated in our *Third Report*) and provide resources consistent with the designated priority of their homeland missions

Some people may suggest that organizing National Guard units with "exclusive" homeland security missions could mean that those units will be moved under the Department of Homeland Security. We disagree. Such a move is not only unlikely, it would not be prudent or consistent with the Constitutional underpinnings or historical precedents for use of the military generally and for the National Guard specifically. We have recommended a structure for using the Guard for "national" missions in a Title 32 status and for establishing certain Guard units with exclusive homeland missions—mutual goals. Nevertheless, the President could find it necessary, because of the magnitude of an attack or other circumstances, to bring National Guard units into a Title 10 status to serve with other Title 10 active and reserve forces under Federal command. For such a contingency, all National Guard forces, including those with exclusive homeland security missions, will need to continue to be trained and equipped through the Department of Defense.

Moreover, the governors of the several States should be consulted on the best possible structure and method to implement all of these recommendations that pertain to the National Guard.